Defense Information Systems Agency

Defense Information Infrastructure Services for the Defense Travel System Request for Proposal

June 11, 1997

TABLE OF CONTENTS

Page

1. INTRODUCTION

In early 1995 the Deputy Secretary of Defense directed the implementation of a Travel Reengineering task force recommendations for sweeping changes to the way DoD goes about the travel process and charged the Under Secretary of Defense Comptroller with the reengineering effort. The Vision is to have a seamless, paperless system that will meet the needs of the traveler, commanders, management and process owners; it must reduce cost, support mission requirements and provide superior customer service.

In December 1995 the Defense Travel System (DTS) Program Management Office (PMO) submitted a "Solicitation for Information or Planning Purposes" to industry for comment. Approximately 220 questions were returned requesting among other things additional information about Electronic Commerce (EC), the Defense Message System (DMS), and the Defense Information Systems Network (DISN). All these components are part of the Defense Information Infrastructure (DII).

1.1 Background

The Defense Information Systems Agency (DISA) has program oversight for the DII. Included in the DII are:

- the DoD Electronic Commerce Infrastructure (ECI) for handling EC/EDI transactions between DoD and its trading partners;
- the DMS, which will provide a global interoperable seamless electronic mail system using commercial off-the-shelf products to conduct secure messaging throughout DoD;
- the Unclassified Internet Protocol Router Network (NIPRNET), which is that portion of the Defense Information System Network (DISN) for handling unclassified but sensitive traffic;
- and the Defense Megacenters (DMCs), which consolidate Information Resources Management (IRM) data processing for DoD.

This document will describe the services available for each of these components, including an overview of the DII.

At the request of the DTS PMO, the Defense Information Systems Agency (DISA) developed this document that offerors could utilize to include the DII in their proposed solutions. Included in the document are costs for EDI, DMS, NIPRNET, and DMC support and services that may apply to the DTS and the DTS vendor.

1.2 Purpose

The purpose of this document is to outline the functions and components of the Defense Information Infrastructure (DII) available for use by the Defense Travel System (DTS). It also outlines methods for using these services and any costs to the vendor associated with the use of these services.

1.3 Scope

This introduction provides an overview of the DII and the Global Combat Support System (GCSS).

The remaining chapters provide a descriptive narrative of the following areas and provides information on costs associated with the them and the procedures for using these services:

- ECI, EDI Compliance Testing, Contractor Registration, and EDI Standards
- DMS X.400 Messaging, X.500 Directory Services, Digital Signature Standard (DSS), and Security
- DISN NIPRNET Connectivity and Associated Cost Structure
- Common Operating Environment (COE) and Shared Data Environment (SHADE)

1.4 Description of the DII

The DII is a seamless web of communications networks, computers, software, databases, applications, data and other capabilities that meets the information processing and transport needs of Do D users in peace and in all crises, conflict, humanitarian support, and wartime roles. It includes:

- The **physical facilities** used to collect, distribute, store, process, and display voice, data, and imagery;

- The **applications and data engineering practices** (tools, methods, and processes) to build and maintain the software that allow users to access and manipulate, organize, and digest proliferating quantities of information;

- The **standards and protocols** that facilitate interconnection and interoperation among networks and systems and that provide security for the information carried; and

- The **people and assets** which provide the integrating design, management and operation of the DII, develop the applications and services, construct the facilities, and instruct others in DII capabilities and use.

The Defense Information Systems Agency (DISA) is actively facilitating the migration of information systems and common, standard data into an integrated and interoperable Defense Information Infrastructure (DII), in support of the National Military Strategy and the Command, Control, Communications, Computer, and Intelligence for the Warrior (C4IFTW) concept. DISA is responsible for developing and managing common infrastructure services such as the Defense Information Systems Network (DISN), the Defense Message System (DMS), Information Systems Security (INFOSEC), Electronic Commerce/Electronic Data Interchange (EC/EDI), and the Defense Megacenters (DMCs).

1.4.1 Technical Infrastructure

The Technical Infrastructure of the DII includes the Defense Information Systems Network (DISN) communications base; the Defense Megacenters for handling major information system processing and maintenance; and the DII Control Concept to manage the DII network and systems.

1.4.1.1 Shared Services

Shared services provide cross-functional, cross-organizational capabilities for interpersonal and interorganizational messaging through Defense Message System (DMS), and support electronic Commerce (e.g., procuring, provisioning, shipping, making payments) through EC/EDI. The DII Common Operating Environment (COE) provides a set of integrated common support services and a corresponding software development environment for functional applications. The DII COE provides common services and enables execution and integration of joint and service mission applications. Shared data supports Interoperability of Functional Applications at the data level among Services and functional areas as needed to conduct the DoD’s mission.

1.4.2 Relationship of the DII and the National Information Infrastructure (NII)

The NII is a Federal-level enterprise, in concert with industry, state and local governments, to develop a national high-speed information processing and transfer network. Evolution of the NII includes national telecommunications policy reform to encourage growth of the information industry. The NII is by definition national in scope. The scope of the DII is international.

The DII provides interfaces for DoD customers to other sources in the NII and to U.S. Allies. The DII also can provide information services to selected non-DoD customers. For example, service could be extended globally for NII customers through existing DII capabilities. Also, strategic cooperation between the DII and the NII organizations will foster development of dual-use technologies, technology transfer, information technology standards, and defense conversion to reduce the cost to the government of providing information services while increasing U.S. global competitiveness in information technologies.

1.5 Description of the Global Combat Support System (GCSS)

Lessons learned from Operation Desert Storm pointed to the need for an integrated view of the battlefield for the Joint Warfighter. GCSS will provide the common environment and shared infrastructure that are the necessary building blocks for information exchange and interoperability. Characteristics of the future environment are:

- Common Applications
- Shared data
- Shared hardware and Reusable Software Modules
- Standard Electronic Transactions
- Shared Infrastructure Services

1.5.1 Capabilities Provided by the GCSS

GCSS is a subset of the DII. In conjunction with other DII elements including Global Command and Control System, DISN, DMS, Megacenters, and CINC/Service/Agency projects, GCSS provides the information technology capabilities required to move and sustain joint forces. Each of these elements provide a combination of application, common environment, shared infrastructure, and hardware and software capabilities.

GCSS will provide the following specific technical capabilities:

- Combat Support Applications Integration - services that support the integration of applications and data into the common operating and shared data environments. This includes: application segmentation, database co-hosting, shared database integration, application re-engineering to use the common operating environment, and implementation of the DII integration standard.

- Common Operating Environment - services that support the development of common reusable software modules that enable Interoperability across multiple combat support applications. This includes: segmentation of common software modules from existing applications, integration of commercial products, development of a common architecture, and development of common tools for application developers.

- Shared Data Environment - services that support the implementation and maintenance of data resources that are used by two or more combat support applications. Services provided include: identification of common data, physical data modeling, data base segmentation, development of data access and maintenance routines, and database re-engineering to use the common data environment.

- EC/EDI Infrastructure - the common technical components and services to support electronic transactions across the DoD. Key components include Network Entry Points, Gateways, Compliance Test Facility, Central Contractor Registration, Customer Service Center, and connectivity between all these entities and Value Added Networks.

- Communications Upgrades - the expanded Non-Classified Internet Protocol Router Network (NIPRNET) communications services to support effective data exchange between fixed sites and from deployed forces to the sustaining base. Upgrades include installation of Asynchronous Transfer Mode (ATM) Switches at ten sites, connection to existing Internet Protocol routers at twenty-four sites, leasing of transmission circuits to connect the sites, and implementation of network management services for the ATM backbone.

- Testing and Integration Facility including Continuity of Operations and Processing Surge Support - provides for continuity of operations for GCSS sites.

- Common Hardware Components - services that support the acquisition, delivery and installation of common hardware. Shared hardware includes: database machines with mid-tier servers, application servers, local area network components and wide-area network switches.

Software Enterprise Licenses - services that support the acquisition and delivery of common software. Enterprise licenses will be acquired for operating systems, database management systems, and commercial-off-the-shelf support applications such as word processors.

2. DISA EC/EDI SERVICES

The purpose of this chapter is to outline the functions and components of the Department of Defense (DoD) Electronic Commerce Infrastructure (ECI) services of the Defense Information Infrastructure (DII) available for use by the Defense Travel System (DTS). It also outlines methods for using the ECI, as well as procedures for registering and testing with the ECI. Terms and definitions and references can be found at the end of this chapter.

2.1 Description

The Secretary of Defense, on December 20, 1993, approved the establishment of a DoD standard, centralized Electronic Commerce (EC)/Electronic Data Interchange (EDI) infrastructure. The Defense Information Systems Agency (DISA) was appointed the “Technical Implementer” of the ECI. The ECI is a standards-based communication and computing infrastructure composed of support services and facilities. Developed and operated by DISA, the ECI consists of the Electronic Commerce Processing Node (ECPN), the Central Contractor Registration (CCR), connections to the Compliance Certification Facility (CCF), and communications infrastructure. It supports EC within the Federal Government and between the Government and private industry. Each of these components are explained in this chapter.

DISA developed the ECI to facilitate communication within DoD elements and between DoD elements and other government entities. Its use will ensure that DoD’s and other government entities’ electronic transactions are received by external Trading Partners in a similar manner, regardless of project or service. This means that EDI transactions from different Automated Information Systems (AISs), such as DTS and DoD financial AISs, using wholly dissimilar technologies, can be transmitted through diverse communication means to arrive at the ECI where the transactions are transmitted in exactly the same manner to each Trading Partner (TP) AIS. The intent is not that every process must be identical, but that the process "looks" the same. The objective of the ECI is to:

- Enable the entire Federal Government and its systems to achieve time and cost savings and economies of scale when implementing EC/EDI through the use of a common infrastructure.
- Provide a "single face to industry," i.e., vendors should be able to conduct similar business transactions electronically in the same manner across DoD sites.
- Use Federal Implementation Conventions (ICs) to the American National Standards Institute (ANSI) Accredited Standards Committee (ASC) X12 standards for EDI transactions (and in the future United Nation's EDI for Administration, Commerce and Transport (UN/EDIFACT) standards).
- Use existing Government- and Commercial-Off-The-Shelf (GOTS/COTS) software to the maximum extent possible.

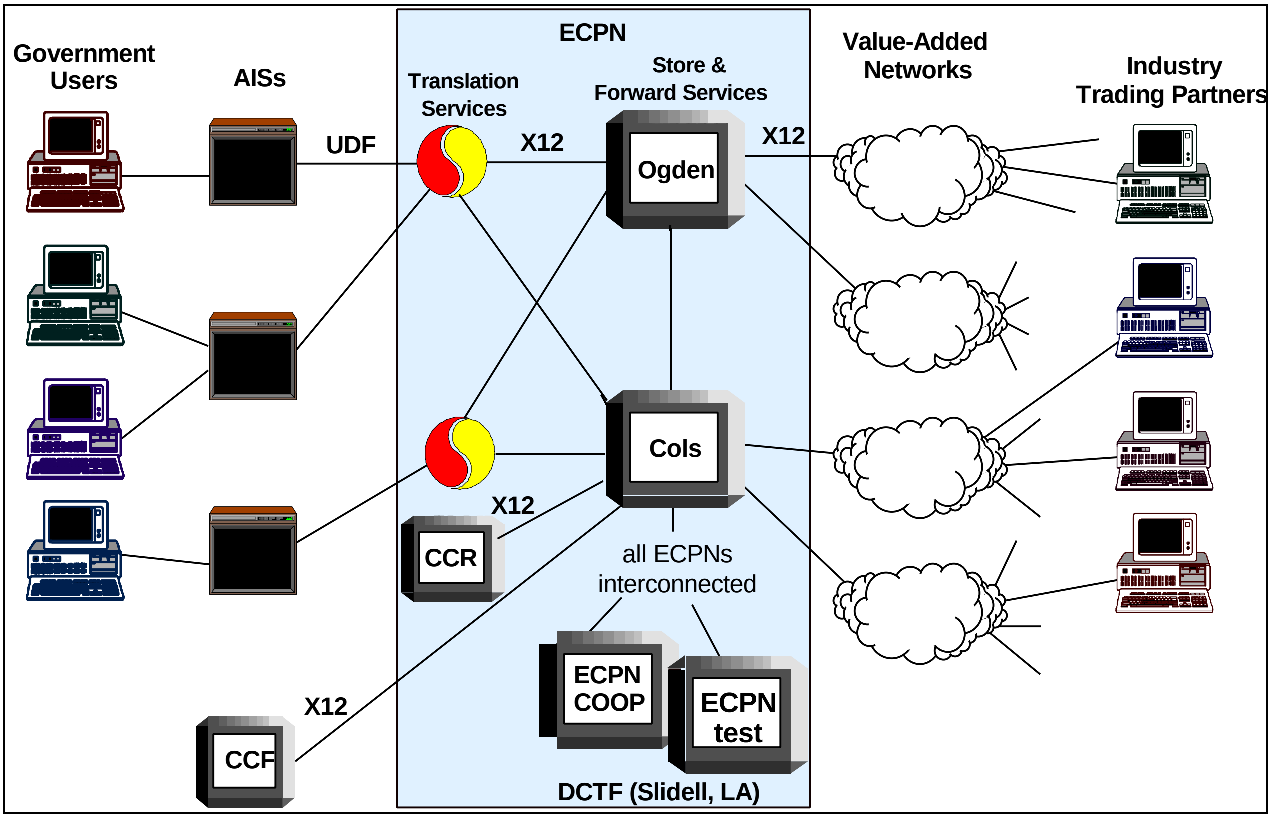
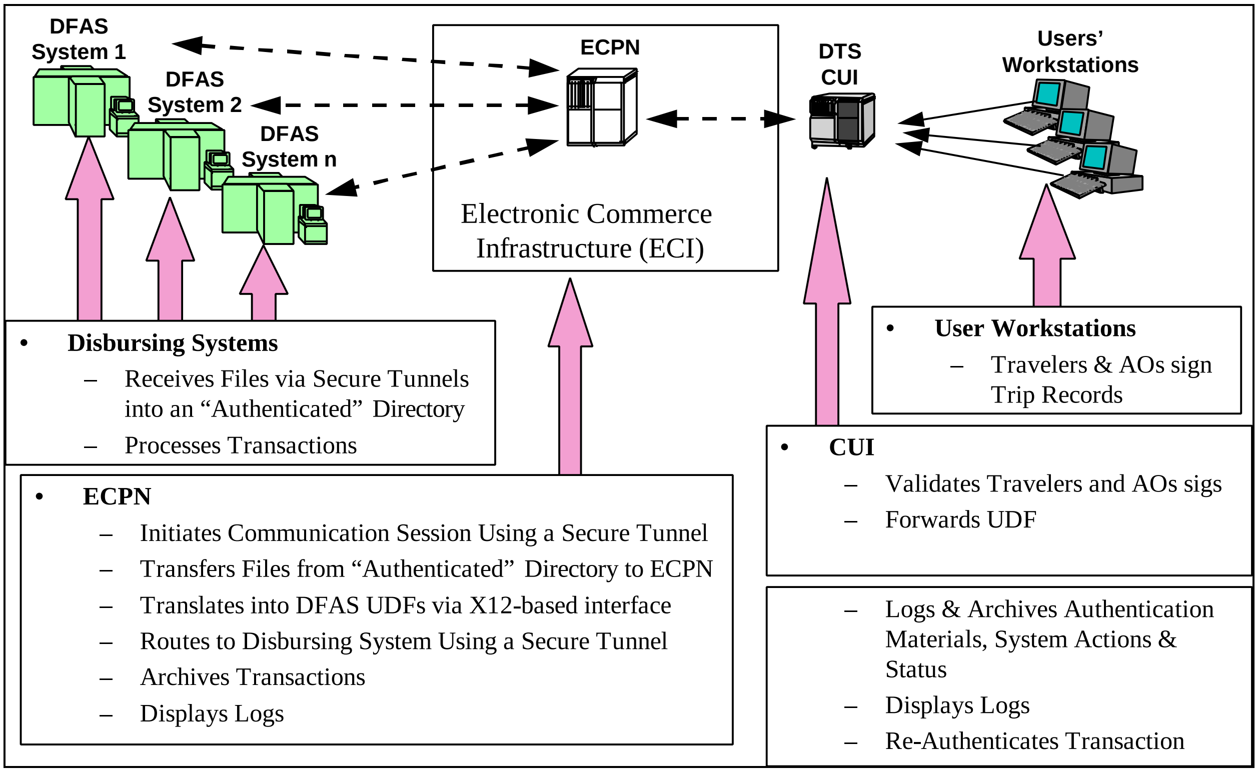


Figure 2-1: Electronic Commerce Infrastructure

Figure 2-1 is a high level overview diagram of the overall ECI. A detailed description of the services that make up the ECI, such as Electronic Commerce Processing Node (ECPN) services, Central Contractor Registration (CCR) services, and the Compliance Certification Facility (CCF) services are contained in the following sections.

The DTS will utilize the ECI to pass financial transactions to DoD financial Automated Information Systems (AISs). The ECPN portion of the ECI cannot be bypassed to pass DTS transactions to DoD financial AISs.



- **Disbursing Systems**
  - Receives Files via Secure Tunnels into an "Authenticated" Directory
  - Processes Transactions
- **ECPN**
  - Initiates Communication Session Using a Secure Tunnel
  - Transfers Files from "Authenticated" Directory to ECPN
  - Translates into DFAS UDFs via X12-based interface
  - Routes to Disbursing System Using a Secure Tunnel
  - Archives Transactions
  - Displays Logs
- **User Workstations**
  - Travelers & AOs sign Trip Records
- **CUI**
  - Validates Travelers and AOs sigs
  - Forwards UDF
  - Logs & Archives Authentication Materials, System Actions & Status
  - Displays Logs
  - Re-Authenticates Transaction

Figure 2-2: Planned DTS CUI Use of ECI

Figure 2-2 shows how the DTS CUI can utilize the ECI. Secure tunnels are discussed in the Security services section.

The DTS CUI will create User Defined Files (UDFs) containing the data for the financial transactions that the ECPN will pick up and transmit over the dedicated DTS NIPRNET connection with secure tunneling for translation to DoD financial AIS UDFs (via an X12-based interface where CUI UDFs are translated into X12 transactions and translated back out to the DoD financial AIS UDFs). The ECPN would use the same dedicated NIPRNET connection to transmit files from DoD financial AISs to the DTS CUI (after the files have been converted to the DTS CUI UDF format).

2.1.1 Electronic Commerce Processing Node (ECPN) Services

The ECPN is the critical component that links the entire DoD ECI environment together. There are two ECPNs; one located at the Defense Megacenter (DMC) Columbus, Ohio, and the other at DMC Ogden, Utah, at Hill Air Force Base (as shown in Figure 2-1).

The Slidell facility in New Orleans, LA, acts as a Continuity-Of-OPerations (COOP) backup site and as a development and test facility for the ECPN and is collectively called the DISA COOP and Test Facility (DCTF). Each ECPN backs the other up and takes over when one ECPN fails. If both ECPNs fail, then the ECPN COOP platform picks up all processing. The ECPN test platform at the DCTF also acts as backup to the COOP platform in case of failure of the COOP platform. There is no reduction in processing capacity since the COOP and test platforms have equivalent computing capabilities to the ECPNs and are dedicated for recovery. Transfer of processing to the DCTF is transparent to AISs. A copy of all transactions exchanged between the DTS CUI and the ECPNs will be automatically sent by the ECPNs to the DCTF for backup.

The communications backbone connecting Columbus, Ogden, and Slidell is an Asynchronous Transfer Mode (ATM) backbone. The ATM backbone provides for 45 Mbps between each of the ECPN locations. A direct connection to the Non-Secure Internet Protocol Router Network (NIPRNET) is maintained as a redundant capability should the ATM backbone fail. The NIPRNET is that portion of the Defense Information System Network (DISN) for handling unclassified traffic and is managed by DISA. NIPRNET core routers are connected at speeds of between 256 kbps and T1.

Any user with Internet access has the potential to connect to the ECI. The use of modems and dial-up connections for asynchronous and bisynchronous communications will be eliminated by the time of DTS deployment. The ECI will rely solely on IP-oriented communication networks.

The outyear architecture will evolve as a supporting common infrastructure evolves. For instance, the Defense Message System (DMS) will be used to provide standard message elements. Use of DMS will be integrated into EC/EDI operations. More transparently, EC/EDI rides whatever transport layer is provided by the NIPRNET. The planned EC/EDI infrastructure beyond FY97 is depicted in Figure 2-3. Refer to the chapters on DMS and NIPRNET in this document for further information on those components.

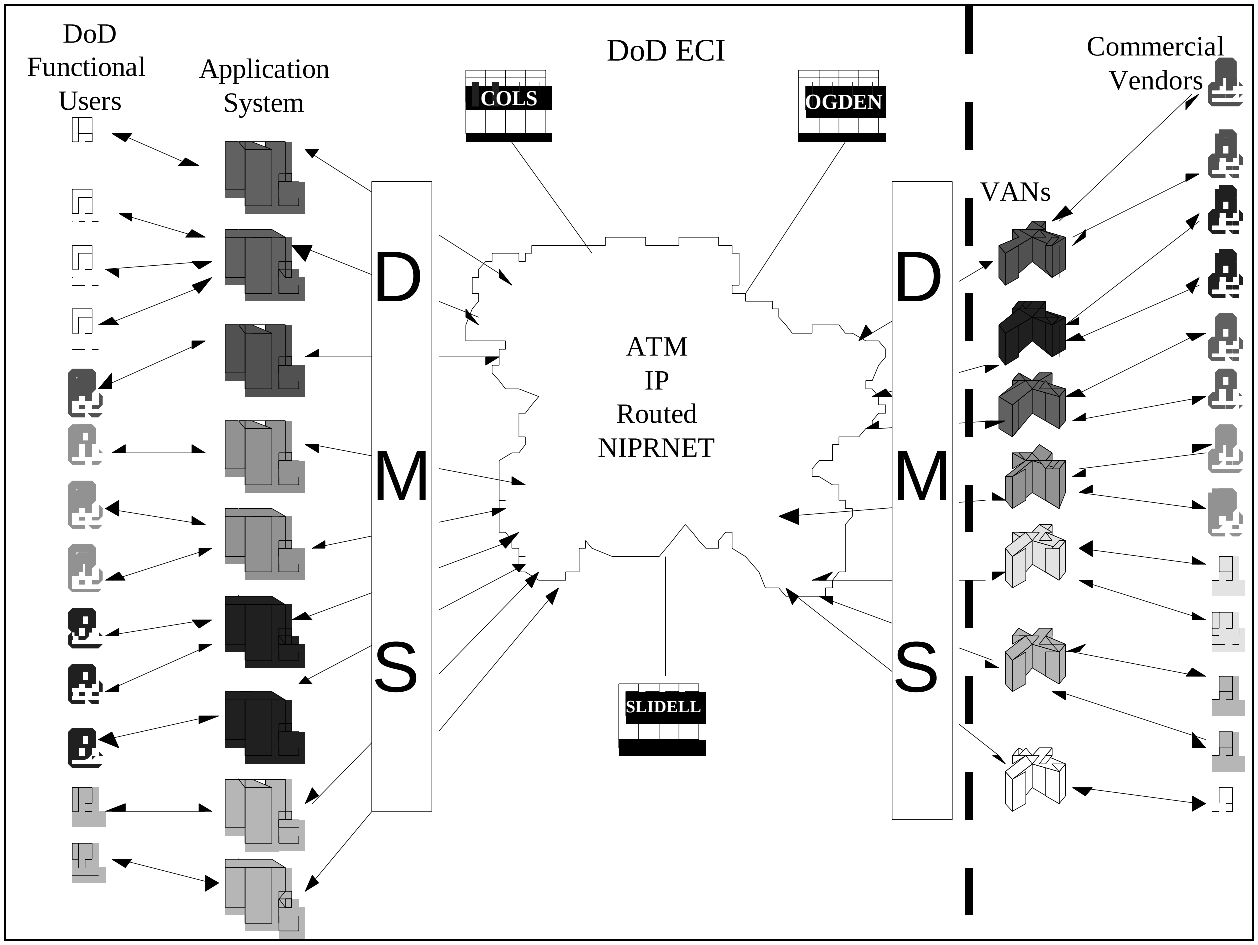


Figure 2-3: Future ECI

ECPN Services include the following:

- Store and Forward services: provides the orderly collection of electronic transactions for distribution to other government activities or Value Added Networks (VANs) for issue to industry Trading Partners (TPs). The ECPN can collect DTS transactions and sort, store, and forward transactions for translation and routing to DoD financial AISs.
- The ECPNs provide, as a minimum, short-term archiving and data recovery capability. This supplies the users (such as the DTS and DoD financial AISs) with an immediate recovery point in case transactions must be retransmitted. Long term archiving and recovery will be the responsibility of the sender of the transaction data.

- Translation services: performs the transaction processing such as translation and enveloping. The ECPNs provide a single point of entry for one or more AISs. The ECPNs provide the ability to change AIS UDFs to the ANSI X12 standard data format and vice versa, in compliance with DoD implementation conventions to the ANSI X12 standards. This helps ensure that the DTS CUI and the DoD financial AISs are passing all the data that the other needs. These services also provide audit information for management and administrator reports. Multiple versions and releases of ANSI X12 standards can be supported simultaneously. The translator can support translation of the data to be exchanged between the DTS and the DoD financial AISs. The ECPN will translate CUI UDFs into DoD financial UDFs and route the transactions to the DoD financial AISs, and vice versa. This is done using an X12-based interface where AIS UDFs are translated into X12 transactions and translated back out into the recipient AIS UDF format. DFAS requires the use of the ECPN to translate DTS files into the specific DoD financial AIS UDF format.

- Environment Manager services: routes data to the AISs (the DTS CUI and DoD financial AISs), and through all the processing points. It also logs all audit information pertaining to the processing of inbound and outbound EDI data between the government agency sites and their TPs (such as DTS and DFAS) to facilitate administration. These services will be utilized to ensure DTS transactions are properly routed to the correct DoD financial AIS site.

- Communications services: uses the DISN, civilian, and commercial networks to exchange transactions between Government agency sites and between each ECPN. The communications module supports unattended operation and error recovery. Communication management reports are provided, such as the number of records transmitted and received from each destination. This module will also support use of X.500 directory services and meet all other requirements of the DMS when available. This module can support routing of transactions between DTS and DoD financial AIS sites.

- Archiving services: provides audit and recovery capability. The ECPN archives all messages received and all log data (incoming and outgoing communications data streams and message logs) and archives them into an Oracle relational database management system (RDBMS). Archiving of transactions received are kept on-line for 45 days for resends. Transaction archives can be held indefinitely off-line and will be determined by DoD financial requirements. Archives of log data are kept indefinitely. Data sent to the ECPN must be retained at the AIS (i.e. DTS CUI and DoD financial AISs) for at least 14 days in case the data must be retransmitted. AISs (such as the DTS and DoD financial AISs) should keep archives of files that are sent out or received by the AIS. The ECPNs will be responsible for archiving files as they are received by the ECPNs and after processing by the ECPNs, before routing to the transaction's destination.

- Directory services: provides addressing information for communications. This directory function will evolve to an X.500-based solution when available from DMS. This module currently can support the specific addressing of transactions to the DTS CUI and DoD financial AIS sites.

- Reporting services: provides ECPN administrators with status and processing information and is provided through log information provided by the translation and/or the environment manager module as a part of its routine operations. Statistics are collected by the ECPN such as file, interchange, and transaction counts and originator/recipient information. Reports containing this information can be forwarded by e-mail as needed.

- Security services: for DTS will include the use of secure tunnels. Tunneling is the method of transporting data between client and server. The client sends a connect request with an identification message encrypted by the server's public key. The server decodes with its private key and sends a response encrypted with the client's public key for mutual authentication. ECPN security services will also support DMS security capabilities when available.

- Digital Signature validation: will only be provided at the DTS CUI for the initial deployment of DTS to Defense Travel Region 6 (DTR6). The ECPN may provide digital signature validation for DTS if future deployments will include end-to-end digital signature between DTS and DoD financial AISs. Again, refer to the PKI/digital signature portion of the DTS RFP for more information.

- Help desk services: provided to assist ECI users with tracking transactions and resolving problems associated with routing and processing transactions (such as those exchanged between the DTS CUI, ECPN(s), and the DoD financial AISs).

2.1.2 Automated Information Systems (AISs)

Automated Information Systems (AISs) are applications currently used by Federal functional business areas and by industry TPs to meet their automated information gathering and processing needs. Each functional business area and TP is responsible for the functional requirements of its respective AIS.

AISs are usually located at information processing sites (such as the DMCs for DoD) that support remote field offices for information gathering and central or distributed processing of the information. Federal AISs and associated field sites will use the DoD, Civilian and commercial networks to transmit UDF data or actual X12 transactions to the ECPNs for EC/EDI services (translation, directory, communications and security).

2.1.3 Automated Information System (AIS) User Defined File (UDF)

The UDF, as output by an AIS, is the bridge between the AISs and the ECPNs. The AIS UDFs contain the data elements necessary for creating EDI transactions. These data elements are formatted by the AIS software such that the ECPNs are able to translate the data from the UDFs into valid X12 transactions. The ECPNs can also reproduce UDFs and X12 transactions for those transactions going to multiple locations. While the software to accomplish this interface may reside on the ECPN, the actual responsibility for data accuracy remains with the AIS business function.

2.1.4 Corporate Telecommunications

The Defense Information System Network (DISN) is the DoD telecommunications network that provides routing and transmission of data throughout DoD. The DISN connects all major DoD AISs to ECPN locations and supports the exchange of EDI transactions. The Non-secure Internet Protocol Router Network (NIPRNET) is the portion of the DISN for handling unclassified but sensitive traffic and is managed by DISA. The NIPRNET provides a high-speed internet working data transport service designed to support open systems and standards. The Defense Message System (DMS) message services run on the DISN and will support the exchange of EDI transactions when available. For more information on the NIPRNET and DMS, please refer to those chapters in this document.

The ECPN supports the following communications protocols:

- File Transfer Protocol (FTP) over Transport Control Protocol/Internet Protocol (TCP/IP)
- Simple Mail Transfer Protocol (SMTP) over TCP/IP

The DTS CUI may connect to the ECI via a direct connect line to the NIPRNET. The ECI requires at a minimum a 56KB line, acquired through a government sponsor. Refer to the chapter on NIPRNET for more information.

The communications sessions between the DTS CUI and the ECPN(s) will be “ECPN push/pull” (ECPN initiates all communications with the DTS to drop off and pick up files). Communications sessions between the ECPN and the DoD financial AISs will also be ECPN push/pull.

2.1.5 Value-Added Networks (VANs)

Commercial VANs are in the business of distributing electronic transactions to a customer base spread internationally. VANs exchange business documents and information between the Government organizations and their industry customers, which are individuals and commercial organizations. The VANs access the Government ECI by communicating with the ECPNs. All VANs interact with the ECI under a common VAN License Agreement. VANs establish their own agreements with their industry customers.

The DTS will not have to become a certified VAN and adhere to the VAN License Agreement to connect to the ECI. However, the DTS must complete many of the same certification procedures that VANs must complete to connect to the ECI. These certification procedures are discussed in a later section of this chapter.

2.1.6 Trading Partner Corporate Processes

The EC/EDI integration process in Figure 2-1 depicts external trading partners and their AISs notionally. It does not advocate setting mandated hardware or software solutions as long as the transactions to/from these TPs are compatible with Federal Implementation Conventions (ICs) to the ANSI X12 standards. This means that DTS CUI and DoD financial AIS UDFs must contain all data required for the ECPN to be able to create complete X12 transactions that conform to Federal ICs. These Federal ICs are discussed in a later section of this chapter.

2.1.7 The DTS CUI Becoming a Trading Partner with DoD Financial Systems

2.1.7.1 Central Contractor Registration (CCR)

The purpose of contractor registration is to inform the Government that a contractor wants to conduct business with the entire Government using EDI. The Federal Government has created a single master registration database to collect contractor information. The registration process provides the Government with the necessary information to exchange EC/EDI transactions with contractors. It is thus the first step in establishing a EDI trading partner (TP) relationship with the Government. TP registration is discussed in this section. TP certification of EDI transactions is discussed later in the “DISA Compliance Certification Facility (CCF)” section.

The primary purpose of contractor registration is to avoid repetitive registrations with each Government office, and also to create an accurate business profile for each business. The secondary purpose is to streamline the acquisition and payment process by collecting standard procurement information. TPs register one time and have their Trading Partner Profile (TPP) shared with all Federal Government agencies.

All TPs must register with the Federal Government before conducting business via EDI with the Federal Government. VANs also cannot transmit transactions between their TPs and the Government until the TPs have become registered and certified for the specified EDI transactions. Government Agency sites may also have to register in CCR in the future. All registrations will be validated before acceptance. An incomplete or inaccurate TPP will be rejected, and the registering TP notified. If fraudulent registration information is submitted, the TP is subject to administrative, civil, and/or criminal penalties.

Currently the CCR database platform receives contractor registration transactions from contractors through the ECPNs. TPs can register electronically in CCR to do business with the Federal Government by submitting the ANSI ASC version 3040 X12.838 Vendor Registration transaction. The TP can also elect to register on-line by accessing the CCR Interface (CCRI) through the CCR World Wide Web (WWW) site at:

http://www.acq.osd.mil/ec/

This registration would qualify them to do business electronically with all Federal agencies, including DoD, and is designed to simplify access to the government acquisition process. Each TP will be assigned a distinctive identification number by CCR. If the TP implements any change (such as a new address, adding new types of X12 transactions or versions, etc.) the TP must update the registration information in CCR.

Before registering, TPs must first have the following:

- A Taxpayer Identification Number (TIN), issued by the United States Internal Revenue Service.
- A Commercial and Government Entity (CAGE) code, administered by the DoD Defense Logistics Agency (DLA) and used in supply management. The Defense Logistics Service Center (DLSC) provides an on-line Web link from the www.acq.osd.mil site for CAGE code registration.
- A Data Universal Numbering System (DUNS) number, developed by the Dun and Bradstreet company and used to identify EC/EDI TPs in both the private and the public sectors of our economy.
- One or more Standard Industrial Classification (SIC) codes, to identify the area or areas in which your company does business. Also important are the Federal Stock Group (FSG) and Federal Stock Code (FSC) numbers used by most Federal agencies to identify the products they are interested in acquiring.

Once the registration has been submitted to CCR, the registration data is held in a suspense file until the DUNS and CAGE numbers are verified, and the vendor has completed compliance testing. DUNS numbers are checked when the ECPN sends the registration information to Dun & Bradstreet. Requests for verification of CAGE are sent by the ECPN to the Defense Logistics Services Center (DLSC). The registration information is also forwarded by the ECPN to the CCF to trigger the compliance testing of transaction sets the vendor wishes to exchange with DoD.

Once all checks are completed, the registrant is provided a Trading Partner Identification Number (TPIN) that permits the registrant to exchange transactions with the ECPN. The TPIN will become a prerequisite for doing business with the Federal Government whether using EC/EDI or manual processes. The X12 838C (Registration Confirmation) is sent to the vendor by CCR (through the ECPN) as notification of registration acceptance and to provide the assigned TPIN. The X12 824 (Application Advice) and the X12 864 (Text Message) is also used to notify the registrant of any problems with the registration. Notification to non-EDI capable TPs is done via mail. The approved registration information is then forwarded to the ECPNs. The ECPNs can then accept and process transactions sent by the registered vendor.

Registration information must be available before a transaction can be delivered. In order for transactions to reach Government Agency sites using the ECI the TP must have a TPP on the ECPN. This will only occur if the ECPNs have received notification of registration and compliance from the CCF and the CCR. There are no other options available. If the TPP is not set up at the ECPNs, transactions may be rejected.

Once a TP is certified and registered, all government activities utilizing the ECI can access the information to build their appropriate TPPs and to ensure they only do business with registered TPs. CCR also provides contractor registration data to Government AISs by sending the registration data to the ECPNs for translation into the AIS' format. The TP information will be required for use by the ECPNs and DoD AISs.

Access the http://www.acq.osd.mil/ec/ web site for more information on the registration process.

It is a requirement that the DTS vendor register with CCR, even if the vendor will only be exchanging UDFs (instead of X12 transactions) with the ECPN. The DTS vendor can register in CCR using the CCRI and can receive registration confirmation via mail. In addition, any travel industry TPs doing business with the DTS for DoD travel must register in CCR.

2.1.7.2 X12 Standards and Federal Implementation Conventions (ICs)

The Defense Information Systems Agency (DISA) is responsible for maintaining Federal Government information technology standards and conventions. The DISA Center for Standards (CFS) is the designated configuration manager for Federal EC/EDI standards (ANSI ASC X12 standards) and Federal ICs to those standards. The DISA Center for Standards coordinates IC requirements for all DoD and Civilian Agencies through the EDI Standards Management Committee (EDISMC) functional area Working Groups (WGs) and builds ICs to fit those requirements.

ICs are standards profiles detailing exactly how the Federal Government (both DoD and Civilian) intends to use a specific standard or group of standards. The DTS and all its TPs must conform to Federal ICs to the X12 standards to be used. Since the DTS will be exchanging only UDFs with the ECPN, the DTS must ensure it creates UDFs with all data required for the ECPN to create X12 transactions that are compliant with the Federal ICs to be used. The ECPN translator mappings supporting DoD financial AISs must also conform to the ICs. The ECI will ensure conformance to the ICs by compliance testing the X12 transactions created by the ECPNs (compliance testing is explained in the next section of this document).

Two new ICs in X12 version 3070 are being developed by the Federal Government financial WG led by DFAS and the DTS program office to meet DoD financial AIS and travel industry requirements. Five ICs in total will be used for DTS and are the following:

- X12 version 3070 821 Financial Information Reporting Transaction: sent from the DTS CUI to the DoD accounting AIS to establish the obligation of funds and is also sent after the travel is complete to adjust for actual cost.
- X12 version 3070 810 Invoice: sent from the DTS CUI to the DoD disbursing AIS to request payment for travel.
- X12 version 3050 820 Remittance Advice: sent from the DoD disbursing AIS to the DTS CUI as notification that payment was made to the traveler.
- X12 version 3050 824 Application Advice: sent from each receiving AIS to the sending AIS only when it is necessary to notify the sending AIS that the receiving AIS could not process the transaction.
- X12 version 3050 997 Functional Acknowledgment: after translation of an X12 transaction, it is sent by the translator to indicate whether the transaction received could be successfully translated.

To aid Government EDI users and their TPs to access approved Federal ICs, the CFS has developed an on-line standards library. The library provides information on approved Federal ICs to X12 standards used by the Federal Government. The library is accessible to organizations both internal and external to the Federal Government on a World Wide Web site (WWW) site:

http://www.antd.nist.gov/fededi

This site is the primary means for conducting EDI activities, and includes ICs, change proposals, coordination, voting, minutes, and Federal Government positions on non-Government standards bodies. The site furnishes the Federal Government and its vendors and customers a means to access and exchange information about standards. The ICs to be used for DTS will be posted to the site after completion of the approval process. The Federal IC for the X12.838 that can be used to register in CCR is currently posted on this site.

2.1.7.3 DISA Compliance Certification Facility (CCF)

The purpose of the CCF is to provide instruction and conduct testing to ensure that every TP adheres to the Federal Government EDI IC compliance requirements. The CCF also tests Federal Government EDI components (ECPN translator services and AISs) for adherence to the same Federal EDI IC compliance requirements. The EDI transactions created by the ECPN in support of translation into DTS CUI and DoD financial AIS UDFs must pass compliance testing for all EDI transactions to be used. The CCF supports all X12 releases as they are adopted by the Federal Government.

A TP who has met and performed successfully the requirements of this compliance testing will have the authority to do EDI business with any Federal Government entity using the transaction set for which the TP has received a compliance validation notification.

The CCF was established by DoD in Columbus Ohio. The facility has tested numerous Value-Added Networks (VANs), TPs, the DoD ECPNs, and Civilian Government translators. The CCF operates during the hours of 8:00 a.m. and 6:00 p.m. (0800 to 1800) Eastern Time, excluding weekends and all federal holidays. Compliance testing information can also be accessed on the World Wide Web at:

http://edi.oti.disa.mil/

2.1.7.4 Certification Testing

In sequence, DISA will coordinate, schedule, and monitor connectivity testing, compliance testing, and workload testing that is required for the DTS to be certified to connect to the ECI. Certification testing consists of:

(1) Site Surveys:

The DTS vendor must complete a DISA Joint Interoperability Test Command (JITC) Requirements List (RL) in order for DISA to engineer and establish the connection between the DTS and the ECI. The Site Survey may include a prearranged on-site visit where the DTS suite of equipment is inspected and evaluated. Additionally, an overall determination of readiness for technical testing by the DTS is made by the Site Survey team.

(2) Connectivity Testing:

The purpose of connectivity testing is to ensure that the DTS and the government can communicate effectively and efficiently. Connectivity testing, fully described in the JITC Connectivity Test Plan is performed in three stages:

- Static Review - DISA reviews the DTS vendor’s questionnaire responses to ensure that the DTS vendor understands and complies with the basic ground rules for connectivity. A basic interconnection test between the DTS and an emulated ECPN establishes a solid framework for the next stages of dynamic testing.

- Dynamic Testing (Emulation Mode) - the DTS communicates with an emulated ECI provided by DISA. This ensures that the DTS can perform the required mandatory and claimed optional services.

- Dynamic Testing (ECI) - the DTS communicates with the specified ECI test ECPN. This ensures that the DTS performs in a manner which does not degrade or adversely affect the overall operations of the government infrastructure. After successful completion of the connectivity testing, the DTS vendor will be directed to proceed to the next phase of testing.

If the DISA JITC concludes that the DTS has failed the test, it will inform the DTS vendor and the DTS PMO that certification testing has been terminated for the specified reasons, and they are not currently qualified to be certified to connect to the ECI.

(3) Compliance Certification Testing

As discussed in an earlier section, ECPN's X12 transactions created from DTS CUI and DoD financial AISs must successfully complete testing for IC compliance by the CCF. Compliance certification testing will commence after the Government and the DTS vendor agrees that both are ready.

The DTS will send test UDFs to the ECPN for translation into X12. These X12 transactions will be sent to the CCF for compliance certification testing.

The test for each individual IC must be successfully completed within 7 calendar days of the test start date. After successful completion of compliance testing, the DTS vendor will be directed by the Government to proceed to the next step in the certification process.

If the CCF concludes that the X12 transactions created by the ECPN from DTS CUI UDFs do not adhere to Federal ICs, it will inform the DTS PMO that certification testing has been terminated for the specified reasons, and the DTS CUI is not currently qualified to be certified to connect to the ECI.

(4) Operational/Production Testing

Upon notification that the ECPN has successfully completed compliance certification testing for DTS transactions, DISA will conduct operational/production testing. The purpose of this testing is to ensure the DTS is capable of handling the requirements of providing routing and storage of files being sent over the ECI.

Upon completion of all tests, DISA will produce a Certification Test Report. This report will contain documentation of the site survey and individual test results, and a determination regarding technical certification for the DTS. DISA will validate test data, make any system changes, software and/or hardware, necessary for actual operations by the DTS. Once these actions are complete, the DTS will be added to the production environment.

For more information on the complete certification process, and for access to documents referenced, access the DISA web site:

http://edi.oti.disa.mil/certify/httoc.htm

2.1.8 Document References and Terms and Definitions

1. Terms and Definitions can be found at the end of this chapter.

2. References can be found at the end of this chapter.

2.2 Cost

No costs to the DTS vendor for ECI services have been identified at this time. Costs for the use of ECI services by the DTS may be borne by DoD. Costs to the DTS for ECI services will be identified at a later date when the information becomes available.

Direct DISN/NIPRNET connection and DMS costs are separately billable costs and are discussed in their respective chapters of this document.

2.3 Access/Use

2.3.1 Procedures

The following are the procedures to be followed (and are in the order they must be followed) if the DTS is to utilize the ECI. Steps a through d can be done concurrently, which will shorten the implementation time:

a. DTS vendor registers with CCR (approximate length of time to accomplish: 1 week if registration contains all information required and the registration has gone through all validation steps with no problems with the data).

b. DISA conducts site survey of the DTS and the DTS vendor prepares site survey questionnaire (approximately one week to accomplish).

c. DISA and the DTS PMO maps the DTS transactions (of the DTS and DoD financial UDF layout to/from X12) and enter into the ECPN translator (approximately two weeks to accomplish, including map testing).

d. DISA develops archiving and secure tunneling capability, and any special tables or scripting necessary to correctly route transactions (approximately four weeks).

e. DISA in coordination with the DTS vendor and the DTS PMO ensures TPPs pertaining to DTS are entered into the ECPN translator (approximately 2 weeks for approximately 27 DoD financial systems and 600 user sites). This data can be entered manually from TP data provided by DFAS or the DoD Services/Agencies, or downloaded from CCR when that capability is available.

f. DISA and the DTS vendor conducts connectivity testing (emulation mode) between a simulated ECI and the DTS platform (approximately 1 week).

g. DISA and the DTS vendor conducts connectivity testing (using actual ECI) between the ECPNs and the DTS platform (approximately 1 week).

h. The ECPN will perform compliance certification testing with assistance from the DTS CUI by translating DTS CUI and DoD financial UDFs into X12 transactions (from each IC to be used) and routing to the Compliance Certification Facility for compliance validation against Federal Implementation Conventions (ICs) to the X12 standards (approximately 1 week).

i. Conduct end-to-end operational/production testing from the DTS to DoD financial systems via the ECPNs (approximately 2 weeks).

j. The total development and testing time may require at least 11 weeks depending on outcome of tests.

2.3.2 Frequency of Service

The ECPNs exchange transactions with VANs and other Civilian EDI platforms once an hour. Currently the ECPNs are down from 0100 to 0300 local time (Eastern Standard Time for the Columbus, OH ECPN and Mountain Time for the Ogden UT, ECPN) for maintenance.

2.4 Service Availability

2.4.1 Implementation Schedule

The ECPN store and forward, translation, environment manager, communications, archiving, directory, reporting, and help desk services are currently operational.

The Compliance Certification Facility is currently operational.

The CCR is currently able to receive 838s that comply with the Federal IC. The CCR Interface (CCRI) on the CCR World Wide Web site is also currently available.

The ability of CCR to automatically add registrations to TPPs on the ECPNs will be available in a later release of CCR; this capability will be deployed in late FY 1997.

The requirement and schedule for secure communications tunneling and digital signature services is being established and is discussed in a separate section of the DTS RFP. Secure tunnels will be in place in time for DTS testing and deployment.

2.4.2 Location

The ECPNs are located at two DISA Defense Megacenters (DMCs):

- DMC Columbus, Ohio (located on the Defense Supply Center, Columbus)
- DMC Ogden, Utah (located on Hill Air Force Base)

2.4.3 Operational Availability

The ECI is available 22 hours a day, seven days a week. Each ECPN is currently off-line for maintenance from 0100 to 0300 local time (Eastern Standard Time for the Columbus, OH ECPN and Mountain Time for the Ogden UT, ECPN)

2.5 Compliancy/Standards

2.5.1 Standards and Conventions Available

Federal ICs are available from the Center For Standards (CFS) web page (referenced in an earlier section of this chapter). ICs for two of the proposed X12 transaction sets to be used for this project, the 821 Financial Information Reporting and 810 Invoice, are currently being developed in X12 version 3070.   These ICs are currently being developed within the DISA CFS EDISMC process by the Financial Working Group to fit travel industry and DoD financial data requirements. They will be available on the CFS web page when approved. The X12 version

3050 ICs for the 820 Remittance Advice, 824 Application Advice, and 997 Functional Acknowledgment will also be used and are currently available on the CFS web page.

2.5.2 Methods to Become Compliant

Refer to the "DISA Compliance Test Facility (CCF)" section discussed earlier in this chapter.

2.6 Limitations/Restrictions

2.6.1 Rules and Procedures to Access the ECI

Requirements to use the ECI must first be coordinated with DISA. Requirements for DTS data to DoD financial AISs are currently being developed by DFAS, DISA, and the DTS PMO.

Compliance testing of the EDI transactions must commence, and must follow the CCF test plan. It is required that only EDI transactions compliant with Federal ICs may traverse the ECI. The CCF Test Plan can be found at http://edi.oti.disa.mil/.

End-to-end testing of the DTS with the ECI must follow DISA certification procedures, available on: http://edi.oti.disa.mil/certify/httoc.htm

Once end-to-end operational/production testing is successful, the DTS is certified to transmit production data with the ECI.

Should the translation software maps, DTS UDFs, implementation conventions, communications, etc., change so that certification status of the DTS is affected, new certification will be immediately required.

2.6.2 Threshold of ECI Services

The ECI is continuously engineered to provide the thresholds necessary to support the user community. Changes or enhancements are formalized through functional requirements definition by the functional customer (DTS PMO) and technical requirements analysis by DISA.

2.7 Capability

2.7.1 Capacity

The ECPN is currently able to process 1GB of data per day, which is based on EDI traffic currently received. However, capacity is continuously reviewed to provide the infrastructure necessary to support the traffic and new customers.

2.7.2 Throughput

Throughput for the ECPN is measured in percent of transactions received from TPs and delivered within 24 hours. The ECPN delivers 99% of transactions in less than 24 hours, with the mean being no transactions taking more than three hours to reach its destination.

Accountability for the ECPN is less than one file in 10,000 not accountable. Accuracy for the ECPN is that no more than one transaction in one million is garbled or undeliverable. Throughput is also continuously reviewed to provide the infrastructure necessary to support the traffic and new customers.

2.7.3 Response Time

Response time required will be provided to DISA through the requirements identification process by the DTS PMO and is usually based on industry standard norms. Response time is continuously reviewed to provide the infrastructure necessary to support the traffic and new customers. Speed of service currently for the ECPN is all transactions traversing the Infrastructure in less than 180 minutes. The mean time is 60 minutes.

2.8 Security

Within DoD, the NIPRNET IP routing and dial-up communications are used to communicate between the AISs and ECPNs. The controlled maintenance of these communications facilities provides some confidentiality of the data transmission. FTP access by remote users is specified by IP address. Additionally, EDI transactions are only accepted by the ECPN from sites with explicitly configured communications channels on the ECPN.

In support of the DTS, the ECI will employ secure tunneling between the DTS CUI, the ECPN(s), and the DoD financial systems.

Firewalls, in conjunction with properly maintained Internet and NIPRNET routers, will be used by the ECI to prevent unauthorized access to the EDI systems from the Internet by filtering traffic that is from an unauthorized IP address (IP spoofing) or destined to an unauthorized port. E-mail spoofing, where the from-address for a received email message is different from the actual sender's address, may result in threats of masquerade and unauthorized message insertion.

An optional ANSI X12.58 security envelope may be provided by the ECI for future deployments of DTS. The X12.58 security mechanism will be supported to provide confidentiality, integrity, and non-repudiation of origin security services for transmission of the EDI transactions. The X12.58 is an ANSI X12 standard that allows for a security envelope to be placed around either the Functional Group (GS segment) of X12 transaction sets or around a single transaction set. The contents of the envelope can be encrypted, digitally signed, or both.

2.9 Points of Contact for More Information

2.9.1 Standards Information

DISA Center for Standards: http://www.antd.nist.gov/fededi

2.9.2 VAN License Agreement and Certification Procedures

DISA Center for Standards: http://edi.oti.disa.mil/certify/httoc.htm

2.9.3 Compliance Certification Facility Information and Testing Procedures

DISA Center for Standards: http://edi.oti.disa.mil/

2.9.4 Basic EC Information and CCR Registration

Electronic Commerce in Contracting (ECIC): http://www.acq.osd.mil/ec/

All other requests for information should be directed through the DTS PMO for answer by DISA.

2.10 EC/EDI Terms and Definitions

Automated Information System (AIS) - applications currently used by Federal functional business areas and by industry Trading Partners to meet their automated information gathering and processing needs.

American National Standards Institute (ANSI) - organization devoted to development of voluntary standards to enhance productivity and international competition of American industrial enterprises.

ANSI ASC X12 - Accredited Standards Committee X12 comprises industry members who create EDI standards for submission to ANSI for subsequent approval and dissemination or for submission to the United Nations Standards Committee for approval of international EDI FACT standards. They develop a series of standards on electronic data interchange that is based on interdependency. This foundation standard defines the syntax of X12 EDI, as well as the data elements, data segments, and control structures.

Application Program Interface (API) - the bridge between the automated information systems and the ECPN.

Archiving - that part of the ECPN which provides audit and recovery capability.

Asynchronous Transfer Mode (ATM) - The communications backbone connecting Columbus, Ogden, and Slidell and provides for 45 Mbps between each of the ECPN locations.

Center for Standards (CFS) - the Defense Information Systems Agency organization responsible for maintaining Federal Government information technology standards and conventions and is the configuration manager for Federal EC/EDI standards.

Central Contractor Registration (CCR) - a single contact point for a business activity for initial registration and compliance/validation testing in order to conduct EDI business with the Federal Government.

Central Contractor Registration Interface (CCRI) - option that a TP can use to register in CCR on-line through the CCR World Wide Web (WWW) site.

Commercial and Government Entity (CAGE) code - required to register in the Central Contractor Registration (CCR) system and administered by the DoD Defense Logistics Agency (DLA). It is used in supply management.

Communications Module - that part of the ECPN that uses the DISN to exchange transactions between the ECPNs and Government agency AIS sites.

Compliance Certification Facility (CCF) - the component of DoD that tests VANs, Value-Added Services and prospective Trading Partners for EDI compliance to Federal Implementation Conventions to ANSI X12 standards. This is a required process for all entities doing business with the Federal Government.

Continuity-of-Operations Plan (COOP) - back-up plan in the event a primary computer operations site has a catastrophic failure.

Commercial-Off-The-Shelf (COTS) - term used to denote commercially available software already developed and ready-to-use.

Common User Interface (CUI) - the DTS platform that will be exchanging EC/EDI transactions with the DoD Electronic Commerce Infrastructure.

Data Universal Numbering System (DUNS) number - required to register in the Central Contractor Registration (CCR) system and developed by the Dun and Bradstreet company. It is used to identify EC/EDI trading partners in both the private and the public sectors of our economy.

Defense Information Infrastructure (DII) - Seamless web of communications networks, computers, software, databases, applications, data and other capabilities that meets the information processing and transport needs of DoD users in peace and in all crises, conflict, humanitarian support, and wartime roles.

Defense Information Systems Agency (DISA) - the DoD agency responsible for providing EC/EDI, DMS, and communications services for DoD Services/Agencies and their automated information systems.

DISA COOP and Test Facility (DCTF) - The Slidell facility in New Orleans, LA, that acts as a continuity-of-operations (COOP) backup site and as a development and test facility for the ECPN.

Defense Information System Network (DISN) - the DoD communications network that provides control, movement, and security of Government electronic data.

Defense Logistics Agency (DLA) - DoD agency that administers Commercial and Government Entity codes.

Defense Megacenter (DMC) - Consolidated data processing centers that provide services to DoD such as technical support for hardware systems, worldwide networks for classified and unclassified operations, system software, and customer applications.

Defense Message System (DMS) - all hardware, software, procedures, standards, facilities, and personnel used to exchange messages electronically between organizations and individuals in DoD.

Defense Travel System (DTS) - DoD-wide system of travel services to be implemented in order to reengineer the DoD travel process.

Department of Defense (DoD) - the customer for the travel services DTS will provide and the developer and operator of the Electronic Commerce Infrastructure.

Directory services - that part of the ECPN that provides addressing information for communications.

EDI for Administration, Commerce, and Transport (EDIFACT) - the international EDI message standard based largely on ANSI X12 standards.

Electronic Commerce Infrastructure (ECI) - a communication and computing infrastructure composed of standard support services and facilities based on standards and principles of open systems. Provides a means of interchanging standard EDI data at a low cost and with a minimum impact on existing automated systems.

Electronic Commerce Information Center (ECIC) - a central office established to act as the primary point of contact for any vendor, or interested governmental entity, desiring to be a Federal Government Trading Partner.

Electronic Commerce (EC) - The business environment created by the application of commercial standards and practices to automate the management and exchange of business and technical information.

Electronic Commerce Processing Node (ECPN) - the main component of the ECI that enables the exchange of EDI transactions between the Federal Government and commercial Trading Partners and also between Federal Government entities.

Electronic Data Interchange (EDI) - the computer-to-computer exchange of data in standard formats. The exchange of routine business transactions in a computer processable format, covering such traditional applications as procurement, transportation, supply, maintenance, and finance.

Electronic Data Interchange Standards Management Committee (EDISMC) - functional working groups containing members from interested DoD and Civilian Agencies that coordinate functional requirements for ICs developed and maintained by the DISA Center for Standards.

Environment Manager services - component of the ECPN that routes data through all processing steps.

Federal Government - term used to refer to both the Department of Defense and Civilian Agencies.

Federal Information Processing Standards (FIPS) - Federal standards issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary of Commerce pursuant to Section III (d) of the Federal Property and Administrative Services Act of 1949 as amended by the Computer Security Act of 1987, Public Law 100-235.

Federal Stock Code (FSC) - required to register in the Central Contractor Registration system and are numbers used by most Federal agencies to identify the products they are interested in acquiring.

Federal Stock Group (FSG) - required to register in the Central Contractor Registration system and are numbers used by most Federal agencies to identify the products they are interested in acquiring.

Government-Off-The-Shelf (GOTS) - term used to denote software already developed by the Government and available for use.

Implementation Conventions (IC) - that portion of EDI implementation guidelines that maps applications data requirements into a specific ANSI transaction set. The Defense Information Systems Agency Center for Standards is the component responsible for ensuring that the Federal Government EDI efforts are consistent with the established EC/EDI architecture in order to present a “single face to industry.”

Joint Interoperability Test Center (JITC) - Component of DISA that is responsible for testing.

NIPRNET - Unclassified Internet Protocol Router Network; the portion of the Defense Information System Network (DISN) for handling unclassified but sensitive traffic.

Public Key Infrastructure (PKI) - means to electronically verify the identity of a message sender based upon the senders’ public key certificate, verify message integrity and detect message alteration, exchange keys for confidentiality, authenticate identity based on a public key certificate, and specify subject attributes such as security clearance and privileges.

Standard Industrial Classification (SIC) Codes - required to register in the Central Contractor Registration (CCR) system and are used to identify the area or areas in which a company does business.

Taxpayer Identification Number (TIN) - required for registration in the Central Contractor Registration (CCR) System and are issued by the United States Internal Revenue Service.

Trading Partner (TP) - any customer, supplier, or service provider (e.g., bank, manufacturer) that conducts business with a Federal Government entity and is involved in the exchange of EDI transmissions. It can also denote Federal Government entities exchanging transactions with each other.

Trading Partner Identification Number (TPIN) - provided to the vendor upon successfully registering with the Central Contractor Registration (CCR) system and permits the registrant to exchange transactions with the ECPN.

Trading Partner Profile (TPP) - developed from the TP registration in CCR and contains TP information required to address X12 transactions at the ECPN so they can be routed to the correct recipient.

Transaction Set - definition, in the standard syntax, of information of business or strategic significance. Consists of a transaction set header segment, one or more data segments in a specified order, and a transaction set trailer segment.

Translator - any program or product that converts a trading partner’s existing file into EDI transactions. It also validates the file and establishes internal acknowledgments for the trading partner. It is the portion of the ECPN that converts the AIS data format to ANSI X12 standard data format and vice versa.

User Defined File (UDF) - contains the data elements necessary for creating EDI transactions. It is output from an AIS and is the bridge between the AISs and the ECPNs.

Value-Added Network (VAN) - a public or private packet-switched network that provides a variety of services which allows Trading Partners to have one communication environment; a communications network that transmits, receives, and stores EDI messages for EDI trading partners.

VAN License Agreement (VLA) - The agreement between VANs and DoD allowing the VAN to connect to the ECI after all certification procedures have been met.

World Wide Web (WWW) - a network of Internet sites where information on the Federal Government EDI program can be obtained.

X12.58 - the ANSI X12 standard that allows for a security envelope to be placed around either the Functional Group (GS segment) or a single transaction set of an X12 transaction set.

2.11 EC/EDI References

DoD Directive 5000.1, “Defense Acquisition”, 15 March 1996; available at http://www.acq.osd.mil/api/asm/

DoD 5200.1-R, *Information Security Program Regulation*, 15 March 1996; available at http://www.acq.osd.mil/api/asm/

DoD Electronic Commerce (EC)/Electronic Data Interchange (EDI) in Contracting Report, DUSD(AR) Electronic Commerce in Department of Defense Small Procurement Process Action Team (PAT), 20 December 1993. It can be obtained from the Government Printing Office by calling 202-512-0132 and asking for stock number 008-000-00643-1, or by accessing the WWW site at: http://www.access.gpo.gov/su_docs/

It is also available from the Defense Technical Information Center (DTIC) WWW site: http://www.dtic.dla.mil and via anonymous FTP at: asc.dtic.dla.mil

Federal Information Processing Standard Publication No. 161 (FIPS PUB 161) "Electronic Data Interchange," 29 March 1991. It is available from the National Technical Information Service (NTIS) by calling 703-487-4650 and asking for NTIS accession number FIPS PUB161-1 (the cost is $12.50). The document discusses the Federal Government’s intent to use ANSI X12 standards for EDI.

Presidential Memorandum for the Heads of Executive Departments and Agencies/The Presidents Management Council, subject: "Streamlining Procurement Through Electronic Commerce," 26 October 1993. It can be obtained from the FedWorld BBS, at 703-321-3339 and downloading ecat.exe from the misc library. The WWW site is http://www.fedworld.gov

Other sources of information:

General Services Administration offers a wide range of information including information on EC/EDI. Their WWW site is http://www.gsa.gov/

Data Interchange Standards Association (DISA), the ANSI X12 Secretariat, 703-548-7005; provides ANSI X12 standards-related membership, training, and conference information. The WWW site is: http://www.disa.org

ANSI X12 standards published by the Data Interchange Standards Association may be obtained by calling 1-800-972-4334.

3. DMS SERVICES

3.1 Description

The Defense Message System (DMS) is the replacement system both for AUTODIN and for E-mail currently used by the Department of Defense (DoD). It is a personal computer application, just like any word processor or spreadsheet program that exists on a workstation today. As DMS is implemented throughout DoD, it will be the mandatory system for sending secure messages. The DMS global architecture utilizes system using off-the-shelf products, X.400 messaging protocol with X.500 directory services and an encryption methodology based on the FORTEZZA crypto-card system to conduct secure messaging throughout DoD.

DMS is a system that uses new E-mail technology to increase the speed and capacity of messaging. DMS will also add reliability, security and world-wide directory capability that has applicability to many other information systems. Though having served the country well, current organizational messaging is old, expensive to operate and maintain, and semi-automated at best. DMS is the way the next generation of a secure messaging system will be modernized. The final implementation of DMS will result in a global interoperable seamless electronic mail system using commercial off-the-shelf products to conduct secure messaging throughout DoD.

For a more detailed description of each of the various components that make DMS possible, refer to section G. Capability of this chapter.

3.2 Cost

The usage of the DMS infrastructure is of no cost to the vendor; the government services and agencies share the infrastructure cost. All Non-Federal Government entities interested in purchasing DMS products may contact the DMS contractor Lockheed-Martin Federal Systems directly to negotiate their own contractual procurement of DMS products.

3.3 Access/Use

Personnel must be registered as a DMS Individual and or Organizational User before they can send or receive a DMS Message. It is important to recognize that many of the functions necessary for DMS registration are already being performed today within the confines of a base, post, camp or station’s support staff, i.e., E-mail administration, security administration and in-processing billets. The Certificate Authority Workstation (CAW) functions as the special purpose, trusted workstation that can be used to assign Directory Names and create X.509 certificates. As part of the process, the CAW application initializes each user’s FORTEZZA Crypto logical Card with a Personal Identification Number (PIN) key material, X.509 certificate(s), and selected DMS Information.

DMS User Agents require the use of TCP/IP to support the Directory Access Protocol for X.500 Directory Services. The Advanced Functionality Microsoft Exchange client and the Lotus clients (Notes Express, Fullnotes) can use the TCP/IP stack provided by several Network Operating Systems Such as Banyan Vines and Novell’s NetWare to Support DMS Messaging. In cases where LAN connectivity does not yet exist, the contract offers a variety of communication stacks mapped to platform will utilize the Microsoft Windows TCP/IP stack.

3.4 Service Availability

DMS will be available on a 24 hour x 7 day basis.

3.5 Compliancy/Standards

The DMS Message Handling System and directory services are defined respectively by the X.400 and X.500 standards recommended by the International Telecommunications Union-Telecommunications Sector (ITU-T). The requirements that DMS satisfies are as stated in the Multi-command Required Operational Capability (MROC 3-88) and the Required Operational Messaging Characteristics (ROMC) dated 4 May 1993. The required capabilities are:

- Connectivity / Interoperability
- Guaranteed Delivery / Accountability
- Timely Delivery
- Confidentiality / Security
- Sender Authentication
- Integrity
- Survivability
- Availability / reliability
- Ease of Use
- Identification of Recipients
- Message Preparation Support
- Storage and Retrieval Support
- Distribution Determination and Delivery

The ROMC further details the characteristics required to meet these functional requirements. Together, the MROC 3-88 and ROMC provide the basis for DMS testing. In addition, DMS will comply with the Allied Communications Publication (ACP), ACP123, ACP133(Draft), ACP 120 (Draft) standards, by which U.S. and allied forces will be able to communicate across national domains.

3.6 Limitations /Restrictions

3.6.1 Messaging Limitations

Using the Multifunction Interpreter (MFI), DMS is designed to be interoperable with other E-mail systems using Simple Mail Transfer Protocol (SMTP), commercial X.400 standard, or the JANAP 128 military message protocol (such as AUTODIN). Users will be limited to exchanging E-mail with systems using one of these standards, which includes most current systems.

3.6.2 Security Limitations

DMS use is restricted to registered users with valid FORTEZZA cards. To protect the integrity and ensure the authenticity of DMS messages, DMS security policy requires that all messages be electronically signed and encrypted, regardless of security classification. The technology selected to achieve this security objective requires the use of a FORTEZZA cryptographic card encoded with the user's unique identity and registration data. Users must also enter a Personal Identification Number (PIN) each time the software application is opened. DMS registration is conducted by Organizational Registration Authorities, who certify users' identities and access requirements, in conjunction with Certification Authorities, who program and issue the FORTEZZA cards to users based on their security clearance and "need to know." Without a valid FORTEZZA card, users cannot access DMS to send or read messages. (An exception has been made for the American Red Cross, which is not part of the DoD but supports military members by providing communication services in cases of medical or family emergencies. The Red Cross will be allowed to send and receive DMS messages without signing and encrypting with the FORTEZZA card.) Users can exchange messages with those outside the DMS, but the integrity and authentication services do not have the same high level of assurance without the writer-to-reader security within DMS.

3.6.3 Directory Limitations

Use of DMS, as with any E-mail application, requires knowledge of the recipients' E-mail addresses. Use of DMS security services also requires access to senders' and recipients' security certificates. While it is possible to obtain addresses directly from recipients or other sources, use of the security services requires access to the electronic directory system to communicate with other DMS users. The ability to send E-mail to non-DMS users does not require access to the security data stored in DMS directories (the MFI strips off security data not applicable to users of SMTP or other non-DMS E-mail), but it may be limited by the availability of current E-mail address information.

3.6.4 Hardware and Operating System Limitations

DMS User Agent software will be available in several versions, ranging from a simple, stand-alone E-mail application to advanced functionality packages which combine messaging with groupware features. The type of user agent or groupware suite selected from the available products – as well as any other office automation software also in use at the office workstation – will determine the hardware (memory and processor speed) and operating system required to run the software. A summary of hardware, operating system, and software configuration options is available from the Lockheed-Martin Federal Systems DMS home page at the following worldwide web site:

http://www.dms.loral.com/products/dmsovrvw.htm

3.7 Capability

3.7.1 X.400 Messaging

The Message Handling System (MHS), as defined by ITU-T X.400 Recommendation For Message Handling System (1988), consists of those entities that allow message preparation, submission, transport, delivery, retrieval and storage. Included in the system are User Agents (UAs), Message Stores (MSs), and Message Transfer Agents (MTAs). User Agents act on behalf of end users (which may be individuals, organizations, or other automated processes) to provide the ability to compose and submit messages to the Message Transfer System (MTS). A Message Store stores messages on behalf of a UA much like a mailbox. A Message Transfer Agent moves message through the MTS on a store-and-forward basis, routing messages as required to reach their final destination. These components (UA, MS, MTA) are functional processes that are associated through well-defined interfaces called protocols. For example, the P3 protocol for message submission and delivery defines the interface between the User Agent and the Message Transfer Agent or the MS and MTA. The P7 protocol defines the interface between the User Agent and the Message Store. The P1 protocol defines the interface for passing messages from one MTA to another. The result of using these well-defined interfaces is that components that comply with the standards can interoperate with any other components using the same standard, regardless of vendor. DMS also supports the use of advanced functionality User Agents using client/server architecture to incorporate messaging functions as part of office automation or groupware services, such as Lotus Notes or Microsoft Exchange.

The MHS for DMS also includes several components not covered in the commercial X.400 standard. They include the Multi-Function Interpreter (MFI), for exchanging messages with AUTODIN, SMTP/MIME, and non-DMS X.400 Messaging systems; the Mail List Agent, for creation of message headers for messages addressed to electronic mail lists; and the Profiling User Agent, for dissemination and distribution of messages based on content.

3.7.2 X.500 Directory Services

Directories, such as those based on the ITU-T X.500 Recommendation for Directory Services, are databases that support communications between users by providing the necessary references for names, addresses, and capabilities of participating users and components in the MTS. The X.500 standards define directory services required by X.400 as well as other capabilities required by telecommunications services, which include telephone and telegraph. The key features are user-friendly naming and name-to-address mapping that provide results independent of the location of the user making the query. The components of an X.500 directory are the Directory System Agents (DSAs), which store and process the entries in the database (called the Directory

Information Base, or DIB); the Directory User Agents (DUAs), which allow users to access the DIB, and the Administrative DUAs, which allow users to enter, delete, and update DIB information elements.

The DIB consists of entries for objects defined in the system, and attributes which describe those objects. The objects may be users, groups, network resources, or other items. For messaging applications, these might include individual or organizational names, message system, and security attributes confirming the privileges of an individual or organization. The directory can store not only text, but any information that can be represented in digital form, such as video clips, images, and graphics. The X.500 standards define the interfaces among these components, such as the rules for sharing information and for determining the location of information in a distributed database.

3.8 Security

The security architecture of DMS provides security services to messaging, including integrity, confidentiality, non-repudiation, access control, and authentication. These services are provided using a product from the NSA Multilevel Information Systems Security Initiative (MISSI) program called the FORTEZZA card, a PCMCIA Type II cryptographic card that will be issued to DMS users. The requirement to use the FORTEZZA card for all DMS access is a major difference between DMS legacy messaging systems. MISSI security mechanisms will also be utilized for strong authentication of directory queries. The CAW is used to program the FORTEZZA card and create the security information posted in the DMS X.500 Directory System. Using public key cryptography, the CAW places the user's private key material on the card and creates the corresponding public key material (X.509 security certificate) that will reside in the DMS directory.

3.8.1 Digital Signature Standard (DSS)

The DSS integrity involves the protection against unauthorized or accidental modification, insertion, or deletion of data. The DSS Federal Information Processing Standard (FIPS) 186 was approved in 1994 for Federal agencies & their contractors to use to protect unclassified information when digital signatures are required. It is not intended to encrypt the data in a message, but to assure the recipient of the message's source and the integrity of its contents. It is used when data integrity assurance and data origin authentication is required. Private & commercial organizations can choose to follow the standard voluntarily without paying royalties to the U.S. Government. Copies of this FIPS can be purchased from NTIS at (703) 487-3238. An information fact sheet is also available free from the NIST Publications Office: (301) 975-2791.

3.8.2 Security services provided by DMS and MISSI

Integrity protects against unauthorized or accidental modification, insertion, or deletion of data. Integrity, which is provided by the digital signature capability of the FORTEZZA card, ensures that the content of the message is not changes between originator and recipient.

Confidentiality protects against access or disclosure to unauthorized individuals, entities, or processes. The encryption services of the FORTEZZA card ensure confidentiality.

Authentication and access control provide verification of the identity of users and processes in the system. Enhanced Identification and Authentication, which uniquely identifies each user to the system, is provided by having a user's FORTEZZA card associated with a Personal Identification Number which is required to access the services of the card and DMS applications.

Non-repudiation protects against denial by one of participants in a message exchange or transaction of having participated. The originator of a message cannot repudiate sending it; the recipient cannot repudiate receiving it once delivery has been confirmed. A non-repudiated proof of delivery can be initiated by users by requesting a signed receipt for a message.

DMS, allows users to create, send, receive and store X.400 secure messages, while retaining the features and capabilities of the latest commercial e-mail systems. DMS products will additionally provide for the transfer of text messages, attachments such as graphic and video and ultimately Electronic Commerce and Electronic Data Interchange (EC/EDI).

3.9 Points of Contact

DISA DMS PMO Implementation Manager:

Mr. Tom Clarke, DISA-D2, 703-681-0324, e-mail: clarket@ncr.disa.mil

3.10 DMS Terms and Definitions

Administrative DUA - component of X.500 that allows users to enter, delete, and update DIB information elements.

Authentication and access control - provide verification of the identity of users and processes in the system.

Certificate Authority Workstation (CAW) - functions as the special purpose, trusted workstation that can be used to assign Directory Names and create X.509 certificates.

Confidentiality - protects against access or disclosure to unauthorized individuals, entities, or processes. The encryption services of the FORTEZZA card ensure confidentiality.

Defense Message System (DMS) - replacement system both for AUTODIN and for E-mail currently used by the Department of Defense (DoD).

Digital Signature Standard (DSS) integrity - involves the protection against unauthorized or accidental modification, insertion, or deletion of data.

Digital Signature Standard (DSS) Federal Information Processing Standard (FIPS) 186 - approved in 1994 for Federal agencies & their contractors to use to protect unclassified information when digital signatures are required.

Directories - databases that support communications between users by providing the necessary references for names, addresses, and capabilities of participating users and components in the MTS.

Directory Information Base (DIB) - database component of X.500.

Directory System Agent (DSA) - component of X.500 that stores and processes entries in the DIB.

Directory User Agent (DUA) - component of X.500 that allows users to access the DIB

FORTEZZA card - a PCMCIA Type II cryptographic card selected to achieve DMS security policy, which requires the use of a FORTEZZA card encoded with the user's unique identity and registration data to electronically sign and encrypt all messages regardless of security classification.

Integrity - protects against unauthorized or accidental modification, insertion, or deletion of data.

Message Handling System (MHS) - consists of those entities that allow message preparation, submission, transport, delivery, retrieval and storage.

Message Store (MS) - stores messages on behalf of a UA much like a mailbox.

Message Transfer Agent (MTA) - moves messages through the MTS on a store-and-forward basis, routing messages as required to reach their final destination.

Multilevel Information Systems Security Initiative (MISSI) program - National Security Agency (NSA) service that provides security services to messaging, including integrity, confidentiality, non-repudiation, access control, and authentication through the use of the FORTEZZA card.

Multifunction Interpreter (MFI) - Used by DMS to be interoperable with other E-mail systems using Simple Mail Transfer Protocol (SMTP), commercial X.400 standard, or the JANAP 128 military message protocol (such as AUTODIN).

Non-repudiation - protects against denial by one of participants in a message exchange or transaction of having participated.

P1 protocol - defines the interface for passing messages from one MTA to another.

P3 protocol - for message submission and delivery defines the interface between the User Agent and the Message Transfer Agent or the MS and MTA.

P7 protocol - defines the interface between the User Agent and the Message Store.

User Agents (UAs) - act on behalf of end users (which may be individuals, organizations, or other automated processes) to provide the ability to compose and submit messages to the Message Transfer System (MTS).

X.500 standards - defined directory services required by X.400 as well as other capabilities required by telecommunications services.

3.11 DMS References

The following references and other information can be accessed at the DISA DMS PMO World Wide Web Home Page at : http://www.disa.mil/D2/DMS/

Allied Communication Publication 120 standard (ACP-120)

Allied Communication Publication 123 standard (ACP-123)

Allied Communication Publication 133 standard (ACP-133)

DMS Implementation Schedule

Multi-command Required Operation Capability (MROC 3-88)

Required Operational Messaging Characteristics (ROMC) documents

4. NIPRNET SERVICES

4.1 Description

The Unclassified Internet Protocol Router Network (NIPRNET) is that portion of the Defense Information System Network (DISN) for handling unclassified but sensitive traffic. The network provides a high-speed internetworking data transport service designed to support open systems and standards. It provides long haul routing of the standard DoD Internet Protocol (IP) and, in special cases, is capable of providing the Government Open Systems Interconnection Profiles (GOSIP) specified Connection less Network Service (CLNS). IP is the preferred protocol for use on the NIPRNET. The NIPRNET is an operational network capable of supporting users at the present time and is described in reference 1 in the References section at the end of this chapter.

The NIPRNET also provides a Dial-in Data Service that will allow access to NIPRNET via dial-in asynchronous lines. The access to the NIPRNET is provided by a Communications Server (CS). The modems associated with this service can support line speeds up to 28.8 kbps. Terminal and host devices will be supported. The host is a PC type device that supports the TCP/IP suite of protocols and uses the Serial Line Internet Protocol (SLIP) or the Point-to Point Protocol (PPP) to access the CS. A terminal is a less sophisticated device that utilizes the TCP/IP capabilities of the CS to communicate with hosts on the network. Authentication and Access control are provided by using a fixed User ID and Access Code which will be supplied to each user and which will be check each time a user wishes to access the network. CSs are located throughout the world and a user may dial into any one of the CSs to obtain service.

The Dial-in Data Service is described in the documents listed in the References section at the end of this chapter. The references 1 through 3 listed in the References section at the end of this chapter can be obtained from the Network Information Center (NIC) at:

http://www.nic.ddn.mil/

The dial-in service is depicted in Figure 4-1. A user at a Workstation wants to connect to a Destination Host over the NIPRNET. The user must dial into the CS over the public telephone network. The CS will request the User ID and Access Code. The User ID and Access Code will be sent to the Extended Terminal Access Controller Access Control System (XTACACS) Server by the CS for verification. The XTACACS Server will search the database for this particular User ID and Access Code. If a match is found then the user will be granted access to the NIPRNET and can then establish a connection to the Destination Host.

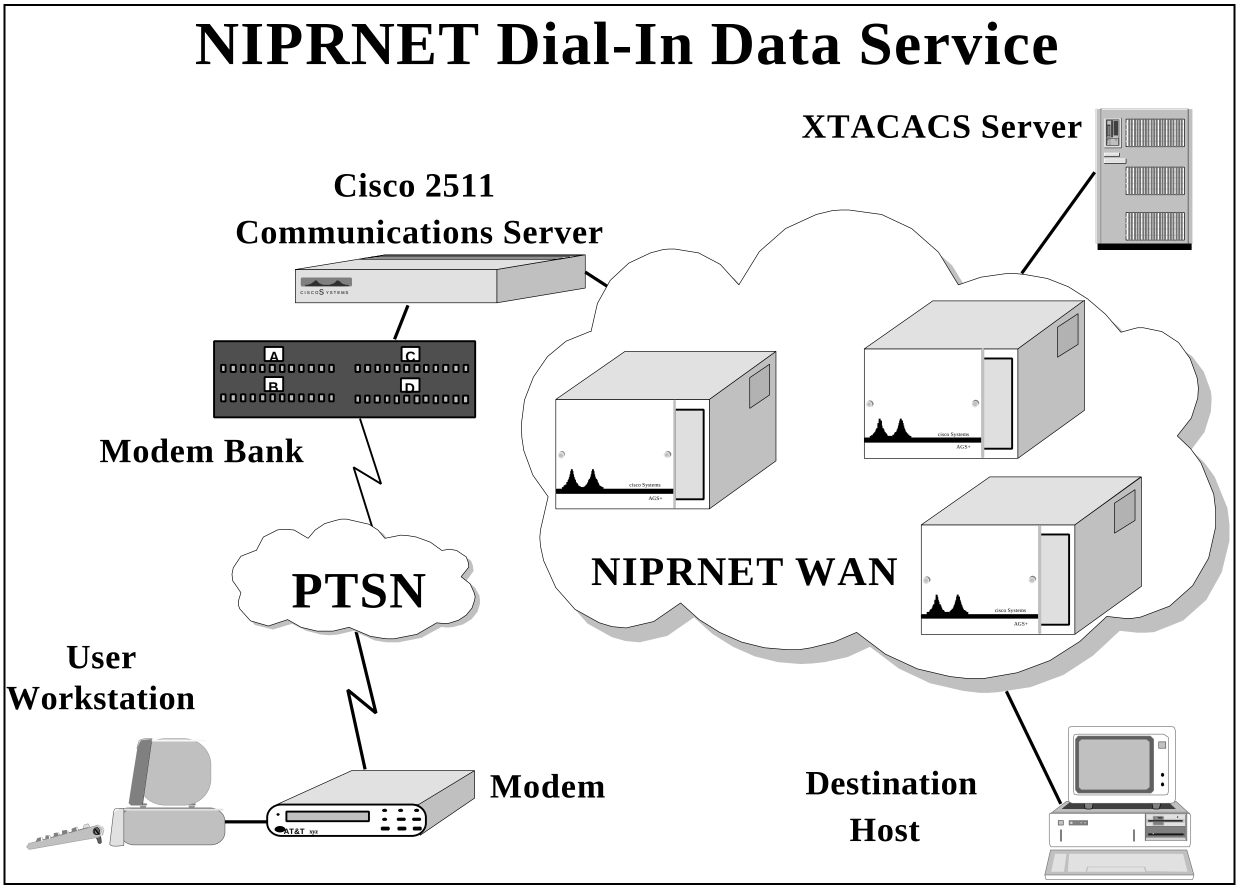


Figure 4-1: NIPRNET Dial In Data Service

4.2 Cost

The costs associated with the use of the NIPRNET for FY1997 are listed in Reference 4 and are shown in Figure 4-2.

The cost associated with a dedicated connection to the NIPRNET is in the form of a one time installation charge and a Monthly Recurring Charge (MRC) which is determined by the speed (128 Kbps, 256 Kbps, etc.) of the access circuit and the Theater of Operation (CONUS, Europe, and Pacific Rim). The access circuit is the connection between the customer equipment and the NIPRNET router. This monthly recurring charge includes the cost of the access circuit, the Channel Service Unit (CSU)/Data Service Unit (DSU), and the Crypto Units used in the OCONUS locations.

The cost of the Dial-in Service is $50 for the initiation fee plus a $27 per month charge for each individual user. This information is also shown in Reference 4 and in Figure 4-2.

IP ROUTER (NIPRNET & SIPRNET) SERVICE

FY97 MONTHLY RECURRING CHARGES

	THEATER:		
BANDWIDTH	CONUS	EUROPE	PACIFIC RIM
ETHERNET (10 MBPS)	$6,749	$9,532	$12,425
9.6 KBPS	1,143	1,173	1,728
16.8-19.2 KBPS	1,104	1,560	2,033
38.4-64 KBPS	1,227	1,733	2,259
128 KBPS	2,047	3,033	3,953
256 KBPS	3,631	5,199	6,777
512 KBPS	5,795	8,665	11,295
1.024-1.544 MBPS	7,322	10,398	13,554
2.04 MBS	N/A	13,864	N/A

ADDITIONAL CHARGES:

NRC FOR INSTALLATION: $2,500 FOR <512 KBPS AND $5,000 FOR > 512 KBPS.

DIAL-UP SERVICE: $50 INITIATION FEE PLUS $27.00 MONTHLY SERVICE FEE.

DUAL HOMING: SECOND CONNECTION OF DUAL HOMED SYSTEM WILL BE CHARGED 50% OF THE MRC FOR THE SPECIFIED DATA RATE.

Figure 4-2: NIPRNET FY97 Monthly Recurring Charges

It should be noted that this is the cost for the user connected directly to the NIPRNET. The user, who is connected to a Base infrastructure, which is in turn connected to the NIPRNET, is a customer of the Base infrastructure and not a customer of the NIPRNET since that particular user has no direct connection to the NIPRNET.

To illustrate this point see Figure 4-3 which shows a subscriber that has 3 locations. Each location contains a premise router which is connected to the NIPRNET via a dedicated synchronous serial line. The premise router is owned and operated by the organization in charge of that site. In this example, there will be a MRC for each of the three connections to the NIPRNET with the cost being determined by the site location (CONUS, EUR, etc.) and the speed of the line. If the three locations are in CONUS and the line speed of each line is 128KBPS then the total monthly cost for this user will be 3 X $2,047 = $6,141. In addition, there will be a one time installation charge of $2,500 for each circuit.

The users connected to the LANs behind the premise routers are the customers of the organization that owns and operates these routers and are not customers of the NIPRNET.

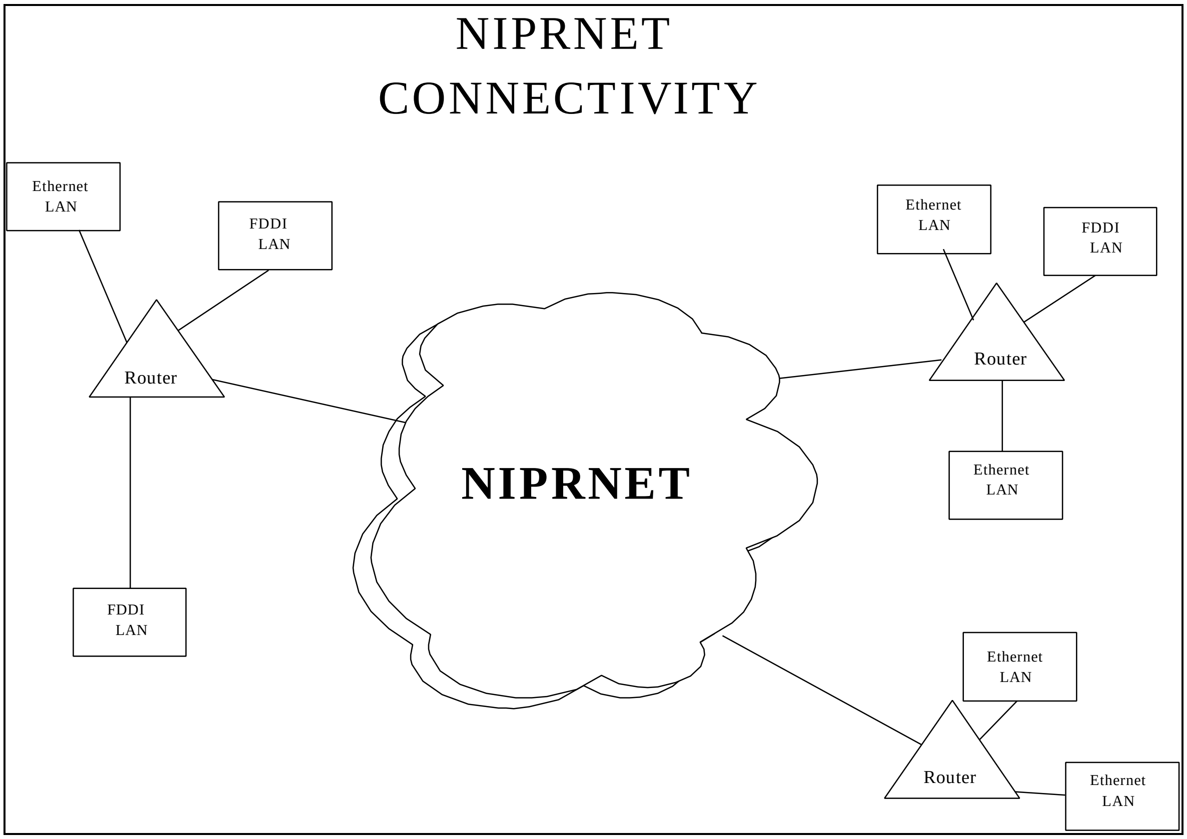


Figure 4-3: Sample NIPRNET Configuration

4.3 Access/Use

The procedures for connection to the NIPRNET are given in Reference 1 - the Router Network Subscriber Guide. The NIPRNET is located in CONUS, Europe, and the Pacific. Connections can be made in any of these theaters. The access line will be run from the NIPRNET router to the customer site. The length of the line is not a concern for the user since the cost of the access line is included in the monthly recurring charge for a dedicated connection.

Based on a US Government contract, authorized contractor personnel may use DOD-controlled systems with access to NIPRNET when performing contractual responsibilities. The sponsoring agency validates and arranges funding for the requirement.

The NIPRNET provides two points of entry/exit to the Global Internet. These points are referred to as the Federal Interconnection Exchanges (FIXs). There is a FIX East and a FIX West where DoD and other Federal and commercial networks interconnect to exchange routing information and provide for Global non-DoD connectivity. These connections allow free flow of data between the NIPRNET and the Internet.

As part of the Integrated Tactical Strategic Data Network program the NIPRNET will support gateways for connectivity to the tactical environments. These entry points are distributed worldwide. Tactical subscribers should employ TCP/IP to access the NIPRNET.

In order to get connected to the NIPRNET the end user must submit a validated Request For Service (RFS) identifying the service requirement to their supporting Telecommunications Certification Office (TCO) in accordance with service/agency procedures. The TCO will assist the user to define all aspects of the requirement.

After the receipt of a validated RFS, the TCO will prepare and submit a Telecommunications Service Request (TSR) as defined in DISAC 310-130-1. The TSR will be forwarded to the Defense Information Systems Agency (DISA) Allocation and Engineering (A&E) activity and other appropriate addressees. The DISA A&E is

DISA
Telecommunications Management and Services Office (TMSO)
Scott AFB, Illinois

A Program Designator Code (PDC) must be included in the TSR. The PDC is specifically required to identify the funding activity responsible for reimbursing DECCO for the cost of the service. DECCO is the Defense Commercial Communications Office, a DISA field activity at

Scott AFB, Illinois. TMSO will submit a Telecommunications Service Order (TSO) to DECCO when leasing action is necessary as well as to identify the use of an existing GFE cable or circuit. A TSO is the authorization from the TMSO to start the procurement process and inform the local Base Communications element of the use of existing GFE cable or circuit.

DECCO will execute the appropriate procurement actions and will coordinate and ensure the delivery of the requested service from the contracted vendor. The lead time associated with the procurement of an access line is approximately 120 calendar days. The lead time denotes the average interval between the receipt of an accurate and complete TSR at the TMSO at Scott AFB and the completion of the action by the communications contractor.

DISA DISN Transmission Support Branch will place the requirement on the Master Schedule as identified in the TSO's Required Service Date. An installation team will be dispatched to the host and the NIPRNET Hub sites to complete the installation.

Columbus Regional Control Center (CRCC) will test the installation and declare it operational upon satisfaction of the customer.

4.4 Service Availability

The NIPRNET router topology has been designed to provide continuous operation with network availability targeted to be at least 99.5% for any pair of single-homed systems. A world wide network management system is maintained 24 hours a day, 7 days per week. Restore times will vary based upon location. A failed network component must be restored within 16 hours for all sites except Alaska, Panama, Spain, Turkey, Guam, Okinawa, and Japan which must be restored within 28 hours.

The actual connection process to the NIPRNET for new remote users will take approximately 90 to 120 days. The speed of the access line must be determined along with the point of entry to the NIPRNET. Then a service order must be placed with the common carriers to obtain the particular circuit.

4.5 Compliancy/Standards

The NIPRNET complies with the Request For Comments (RFCs) that have been developed by the Internet Engineering Task Force (IETF) and maintained by the Internet Architecture Board (IAB). The IAB is responsible for the development of the Internet standards. The necessary RFCs are listed in Reference 5 and can be obtained from the Network Information Center (NIC) at:

http://www.nic.ddn.mil.

The RFCs are contained in the RFC directory and can be accessed by using Aanonymous@ for name and Aguest@ for the password.

Reference 5 (RFC 1920) describes the state of standardization of protocols used in the Internet as determined by the IAB and is updated on a quarterly basis.

4.6 Limitations/Restrictions

The NIPRNET provides support for the Internet Protocol (IP) and some limited support for the Connection less Network Service (CLNS). The NIPRNET does not support the proprietary protocols such as IPX, AppleTalk, SNA, etc. These protocols need to be encapsulated within an IP packet, at a user site, in order to be sent across the NIPRNET and then suitably removed from the IP packet at the other end, again, at a user site. The encapsulation process of the proprietary protocols is the responsibility of the user.

4.7 Capability

The NIPRNET is a high speed wide area network presently operating in CONUS, Europe, and the Pacific. The network consists of a number of routers that are interconnected to one another either by Ethernet for collocated routers or high speed serial links with line speeds of 1.544 Megabits per second. The CONUS portion of the NIPRNET is undergoing a major upgrade (scheduled to be completed by 1 Nov. 1996) which includes a technology insertion to support Asynchronous Transmission Mode (ATM) between selected NIPRNET Core routers at speeds of 45 Megabits per second.

Figure 4-4 shows the Core portion of the target architecture. The ATM sites will over lay the Core and in most cases will be collocated with a Core router. The remaining Core router sites will be connected by dual T1 (1.544MBPS) lines.

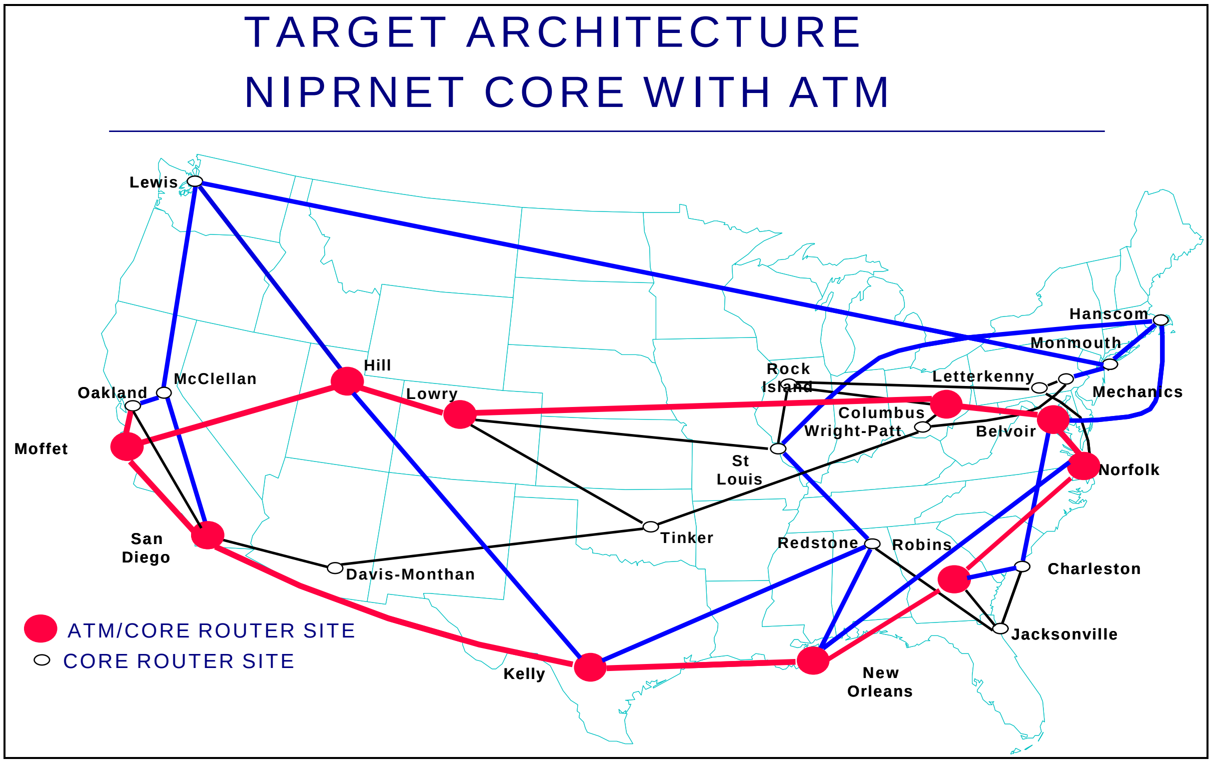


Figure 4-4: NIPRNET Core Portion of the Target Architecture

Figure 4-5 shows the Regional portion of the target architecture. The Regional routers are connected to the Core router and other Regional routers by T1 lines. It is planned to have subscribers connect to the Regional routers.

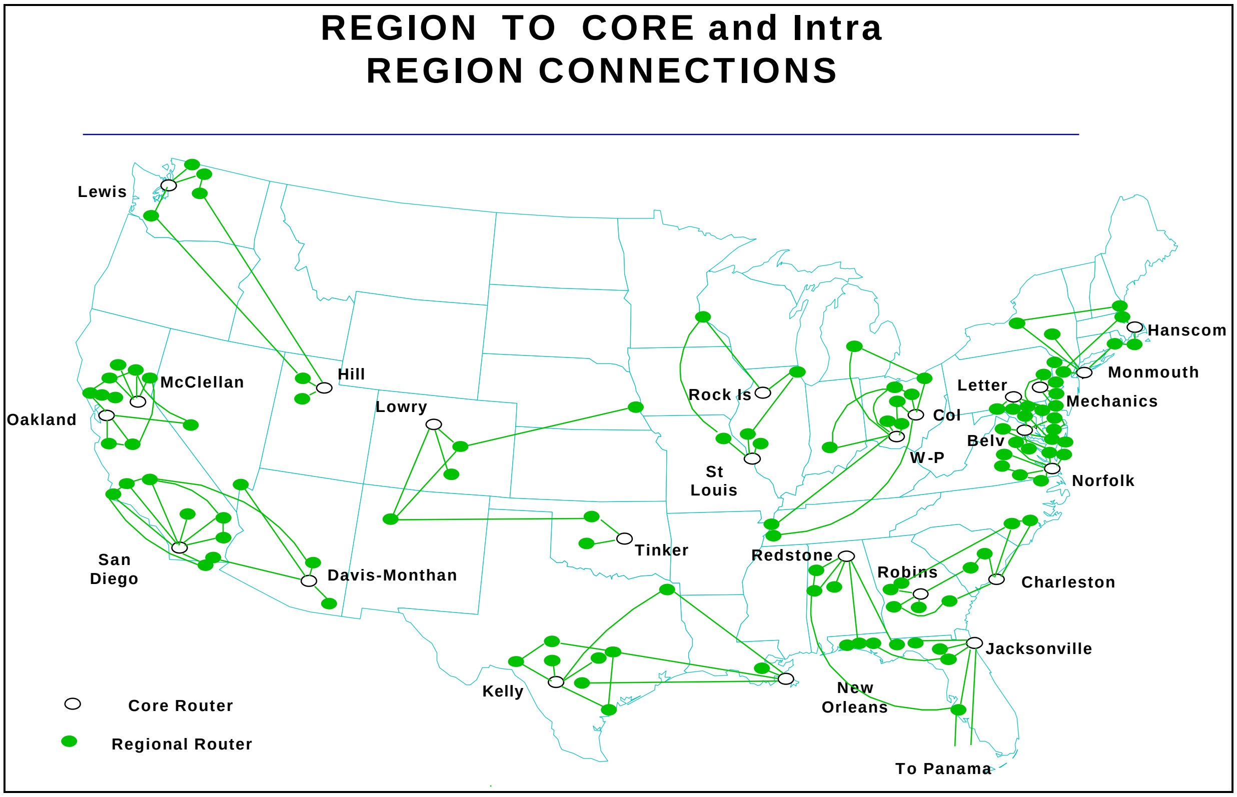


Figure 4-5: NIPRNET Regional Portion of the Target Architecture

The subscribers can connect to the NIPRNET via Ethernet or synchronous serial lines at speeds up to 1.544 Megabits per second.

The design goal for the maximum round trip response time across the NIPRNET is less than 600 milliseconds per 100 Byte packet. This time duration is measured between the source and destination NIPRNET routers.

4.8 Security

Privacy and Security are the responsibility of the subscriber. Subscriber data as it passes through the NIPRNET router infrastructure is not specifically protected. Therefore, if confidentiality is required, the subscriber must implement some form of end-to-end encryption. Limited privacy can be provided by address filtering at the subscriber ports; such implementations must be coordinated with network monitoring center. There is no user security accreditation process associated with the NIPRNET.

For dial up access, the Communications Server will perform identification and authentication for users before allowing access to the NIPRNET.

4.9 Points of Contact

Refer to the Network Information Center (NIC) at: http://www.nic.ddn.mil/

4.10 NIPRNET Terms and Definitions

Communications Server (CS) - provides access to the NIPRNET.

Federal Interconnection Exchanges (FIXs) - two points of entry/exit to the Global Internet provided by the NIPRNET.

Point-to Point Protocol (PPP) - can be used by the NIPRNET host to access the CS.

Serial Line Internet Protocol (SLIP) - can be used by the NIPRNET host to access the CS.

Unclassified Internet Protocol Router Network (NIPRNET) - the portion of the Defense Information System Network (DISN) for handling unclassified but sensitive traffic. It provides long haul routing of the standard DoD Internet Protocol (IP) and, in special cases, is capable of providing the Government Open Systems Interconnection Profiles (GOSIP) specified Connection less Network Service (CLNS).

Extended Terminal Access Controller Access Control System (XTACACS) Server - used by the CS for verification of User ID and Access Code.

4.11 NIPRNET References

1. Defense Information Systems Network (DISN), Router Network Subscriber Guide, 14 Feb. 1995.

2. Defense Information Systems Network, Dial-In Data Service, Service Description & Operational Concept, September 25, 1995.

3. Defense Information Systems Network, Dial-In Data Service User Guide, July 13, 1995.

4. Defense Business Operations Fund, NIPRNET FY 1997 Billing Rates.

5. Network Working Group, Request For Comments: 1920 Internet Official Protocol Standards, March 1996.

5. COMMON OPERATING ENVIRONMENT AND SHARED DATA ENVIRONMENT

5.1 Common Operating Environment (COE)

The Defense Information Infrastructure (DII) Common Operating Environment (COE) originated with a simple observation about command and control systems: certain functions (mapping, track management, communication interfaces, etc.) are so fundamental that they are required for virtually every command and control system. Yet these functions are built over and over again in incompatible ways even when the requirements are the same, or vary only slightly, between systems. If these common functions could be extracted, implemented as a set of extensible low level building blocks, and made readily available to system designers, development schedules could be accelerated and substantial savings could be achieved through software reuse. Moreover, interoperability would be significantly improved because common software is used across systems for common functions.

The DII COE emphasizes both software reuse and interoperability, but its principles are more far reaching and innovative. The COE concept encompasses:

- an infrastructure for supporting mission area applications,
- a rigorous definition of the runtime execution environment,
- a rigorous set of requirements for achieving COE compliance,
- an automated tool set for enforcing COE principles and measuring COE compliance,
- an automated process for software integration,
- a collection of reusable software components,
- an approach and methodology for software reuse,
- a set of APIs for accessing COE components, and
- an electronic process for submitting/retrieving software components to/from the COE software repository.

The DII COE is a "plug and play" open architecture designed around a client/server model. Functionality is easily added to or removed from the target system in small manageable units, called *segments*. Segments are defined in terms of functions that are meaningful to operators, not in terms of internal software structure. Structuring the software into segments in this manner is a powerful concept that allows considerable flexibility in configuring the system to meet specific mission needs or to minimize hardware requirements for an operational site. Site personnel perform field updates by replacing affected segments through use of a simple, consistent, graphically oriented user interface.

To a developer the DII COE is:

- **An Architecture:** A precisely defined TAFIM-compliant (Technical Architecture Framework for Information Management), client/server architecture for how system components will interact and fit together, and a definition of the system level interface to COE components.

- **A Runtime Environment:** A standard runtime operating environment that includes "look and feel," operating system, and windowing environment standards. Since no single runtime environment is possible in practice, the COE architecture provides facilities for a developer to extend the environment in such a way as to not conflict with other developers.

- **Software:** A clearly defined set of already implemented, reusable functions.

- **APIs:** A collection of Application Programmer Interfaces (APIs) for accessing COE components. Thus, the COE is a set of building blocks in the same sense that X Windows and Motif are building blocks for creating an application's Graphical User Interface (GUI).

5.1.1 COE Compliance

The degree to which "plug and play" is possible is dependent upon the degree to which segments are COE compliant. Appendix B of the DII COE Integration and Run Time Specification (I&RTS), contains a detailed checklist for areas where compliance is mandatory, and a checklist for areas where compliance is ultimately required but for which there is room for a migration strategy to achieve full compliance. The COE provides a suite of tools, described in Appendix C of the I&RTS, which validate COE conformance.

The I&RTS is available on the internet with access via the DII COE Home Page:

spider.osfl.disa.mil/dii (Note: it is osf”ell” not “one”)

By its very nature, an exhaustive list of "do's and don'ts" is not possible. COE compliance must be guided by overarching principles with checklists and tools to aid in detecting as many problem areas as possible. Full COE compliance embodies the following principles:

- All segments shall comply with the guidelines, specifications, and standards defined in this document and related documents such as the *Style Guide*.

- All software and data shall be structured in segment format. By definition, COTS components of the bootstrap COE are exempted from this requirement.

- All segments shall be registered and submitted to the on-line library. The registration process is described in Appendix E of the I&RTS while submission of segments to the on-line library is described in Chapter 7 of the I&RTS.

- All segments shall be validated with the VerifySeg tool prior to submission, and shall successfully pass the VerifySeg tool with no errors. An annotated listing of the VerifySeg tool output shall be submitted with each segment release.

- All segments shall be loaded and tested in the COE environment prior to submission. Segment developers are responsible for testing their segment within the full COE, but there is no requirement to include mission application segments for which there is no dependency.

- All segments shall fully specify dependencies and required resources through the appropriate segment descriptors defined in Chapter 5 of the I&RTS.

- All segments shall be designed to be removable, and tested to confirm that they can be successfully removed from the system. Some segments, especially COE components, are designed to be "permanent" but even these must be removable when a later segment release supersedes the current one.

- All segments shall access COE components only through the published APIs, and segments shall not duplicate functionality contained within the COE. There is no requirement to integrate to COE functionality which is not required by the segment, but note that use of some segments may have an implied dependency on other segments.

- No segment shall modify the environment or any files it does not own except through environment extension files or through use of the installation tools provided by the COE.

Applications are measured for compliance to the DII COE in eight levels. They are:

Level 1: Standards Compliant

- Superficial level in which proposed capabilities share only a common set of Government or Industry standards

Level 2: Network Compliant

- Two capabilities coexist on the same LAN but on different CPU

- Limited data sharing is possible

Level 3: Workstation Compliant

- Environment conflicts have been resolved so that two applications may:

1. Reside on the same LAN
2. Share data
3. Coexist on the same workstation

Level 4: Bootstrap Compliant

- All applications are in segmented format and share the bootstrap COE

Level 5: Minimal COE Compliance

- All segments share the kernel

- Functionality is available through the Kernel's Executive Manager

Level 6: Intermediate Compliance

- Segments utilize existing account groups

- Reuse of one or more core component segments

Level 7: Interoperable Compliance

- Interoperability ensured via reuse of all core components segments

- May duplicate other functionality not in the core COE

Level 8: Full COE Compliance

- Proposed new functionality is completely integrated into the system

- Available to COE Executive Manager

- Does not duplicate functionality core COE or other DII segments

Level 5 is considered the initial target level. All new DoD systems must achieve Level 5 compliance; therefore, the DTS CUI should be proposed as a Level 5 or higher system. The compliance levels are explained in more detail in the I&RTS, available on the DII COE Home Page.

5.1.2 How to order the DII COE

The DII COE can be ordered by completing the order form on the DII COE Home page and submitting the completed form to the Defense Computer Testing Facility, Configuration Management, Slidell, LA. Private sector requests must be accompanied with a DOD sponsor's signature.

5.2 SHAred Data Environment (SHADE)

SHADE is a strategy and mechanism for data sharing that represents an extension of the principles of the DII COE. SHADE includes:

- Data Access Architectures

- Data Sharing Approaches
- Reusable Software and Data Components

  Guidelines and Standards

SHADE creates the tools and environment for the development and migration of systems that meet the user's requirements for timely, accurate, and reliable data. Shared Data Environment - services that support the implementation and maintenance of data resources that are used by two or more combat support applications. Services provided include:

- identification of common data
- physical data modeling
- data base segmentation
- development of data access and maintenance routines
- database re-engineering to use the common data environment.

SHADE, like the DII COE, is based upon reusing predefined and already developed data segments. Applications engineered using SHADE data segments will provide applications with access to tested data which represent live representations of the most common (universal) data. These universal data segments will include the data elements and be updated from the authoritative source as changes occur. Applications, therefore, using SHADE data segments will improve data quality and be assured access to the latest versions of data.

5.2.1 Data Segments

Data segments consist of the data’s common business rules, load and install routines, common Create, Read, Update, and Delete statements, and the actual data associated with the data tables represented in the segment.

5.2.2 Registered Segments

Data segments will be registered with the DISA SHADE Lead Engineer and be stored in a repository for access by authorized developers. Registers users of the data segments will be notified when the segment changes so that they may update their applications as needed.

5.2.3 Types of Data Segments

There are three types of data segments:

- Universal data - data used in many applications and systems such as location codes, unit identifications, Zip Code, State and Country codes, etc.
- Shared data - data that is shared between several applications or systems, such as mapping and geodesic data, personnel, financial and procurement/contract specific information.

- Local data - data that is used within the application or system such as flags, triggers, constants, etc.

5.2.4 Conformance with the DoD Data Standards

Data segments shall either conform with the existing DOD data standards or be proposed as additions to the standards. Therefore, applications or systems engineered with the SHADE data segments shall be in compliance with the data standards where segments are used.

The rapid evolution of DII COE and SHADE preclude inclusion of more detailed specifications for vendor consideration. For the latest information, vendors should check the DII COE home page weekly. It is located at: HTTP://www.spider.osfl.disa.mil/dii